عدد خاص
بمناسبة
السنة الأولى

مجلة
مجتمع لينوكس العربي

مجلة تعنى بشؤون المصادر الحرة

العدد ٦ نوفمبر/ ديسمبر ٢٠٠٨

http://www.linuxac.org



إقرأ في داخل العدد:

* من مغامرات المحقق وميرت فونلي: اللغز الغامض للدودة الحمراء!.
* تشفير نظام الملفات/الملفات باستخدام TrueCrypt
* معالجة الصور الرقمية
* القول الحاذق في تثبيت لينكس والمحافظة على النظام السابق
* جنو/لينُكس عالم الحرية .. جنو/لينُكس عالم الطبيعة!
* كيف تستعيد السيطرة على خادمك المخترق!
* والعديد من المواضيع الجديدة والقيمة.

صورة الغلاف: penguincakes

فهرس العدد

كلمة العدد



بسم الله الرحمن الرحيم

عام قد مضى ... وعام سيمضي ... تجربة قد ولدت ... وبدأت تكبر شيئاً فشيئاً ... رضعت من حبر ... وحبت على صفحات من ورق ... وخطت أولى خطواتها بيننا وعلى مرأى من أعيننا ... كبرت وترعرت وتعلمت كيف تنطق أحرفاً وكلمات ... لتسطر بعدها مواضيع ومقالات ... وهاي هي الآن تزهو بثوب جميل ناصع البياض، لتحتفل بالعيدين معاً، عيد أضحى مبارك، وعيد ميلاد تلك الفتاة الجميلة، التي اقتربت من عامها الأول: مجلة مجتمع لينوكس العربي.

بالنسبة للكثيرين منا فإن هذا العدد له صبغة خاصة به دوناً عن بقية الأعداد، فبينما يحتفل المسلمون في أرجاء وطننا العربي والإسلامي بالمناسبة الجميلة العطرة والقريبة من قلوبنا جميعاً ألا وهي مناسبة عيد الأضحى المبارك، فنحن في مجتمع لينوكس العربي لدينا احتفالية من نوع خاص بنا، وهي اكتمال السلسلة الأولى والعام الأول من أعداد مجلة المجتمع، بعد أن ألبسناها ثوباً متميزاً بها، حاكه أعضاء مجتمعنا المتميز، بأقلامهم واجتهادهم وعزمهم على تقديم الأفضل لأبناء أمتنا النائمة والتي تنتظر من يوقظها من سباتها العميق!

وكأي فتاة يافعة تنتظر من يأخذ بيدها للطريق الصحيح، ويوفر لها عيشاً كريماً، ويعلمها ويثقفها ويزيدها معرفةً، فكذلك هو الحال مع فتاتنا الجميلة، المثقفة، الحالمة، نعم .. نريدها ينبوعاً لا ينضب من العلم والمعرفة، نريدها فتية قوية، تتصدى للمترصدين بها، وتقف شوكة في حلوق من يريد بها سوءاً. نريدها جميلة رائعة تبهر من ينظر إليها، وتثير الحسد في قلوب الراغبين في وأدها في مقبرة التاريخ، تلك المقبرة التي امتلئت بشواهد قبور سابقاتها!

هنيئاً لكم بما قدمتم، وهنيئاً لأمتنا بما أخلفتم، قد وصلنا للسنة الأولى بعد جهد وتعب كبيرين، وسنبقى نواصل المسيرة بجهودكم و بمساندتكم لنا، عسى أن نكبر وتكبر فتاتنا الجميلة، ونحتفي بها يوماً ما حين نراها تزف إلى كل فرد من أفراد أمتنا العربية من مشرقها إلى مغربها.



رئيس التحرير

أخبار متفرقة

إعداد: مسلم عادل



صدور اصدار جديد من كتاب Linux from scratch (لينوكس من الصفر في ترجمة حرة).

أعلنت مجموعة Linux From Scratch عن صدور اصدار جديد لكتابهم Linux From Scratch والذي يحمل الرقم6.4.

يغطي هذا الاصدار النواة 2.6.27.4 وGCC 4.3.2 و glibc 2.8 بالاضافة الى مواضيع تتعلق بالحماية والأمان.
لمعرفة المزيد من خلال الرابط:

http://www.linuxfromscratch.org/lfs/view/6.4/

صدور Ulteo Open Virtual Desktop

Ulteo شركة متخصصة في محاكاة (virtualization) البرامج ليتم استخدامها عبر الانترنت اعلنت عن منتج جديد وهو Open Virtual Desktop.

وكما يوحي الاسم، فان Open Virtual Desktop عبارة عن سطح مكتب مفتوح المصدر يعمل من متصفح الانترنت بحيث يستطيع اي شخص استخدامه والاستفادة من تطبيقاته.

تحديث نظام تشغيل iPhone

أعلنت أبل عن اصدار جديد من نظام التشغيل الخاص بـ iPhone والاصدار يحمل الرقم ٢,٢ وشمل على تصحيح بعض الاخطاء ومزيد من التحسينات في النظام وبعض الاضافات. ومن الاضافات الجميلة (والتي للاسف لا تعمل سوى في بضع دول) هي Street View التابعة لـ Google Maps والتي تسمح بالحصول على معلومات عن الشوارع مثل اماكن النقل العام والاتجاهات.

صدور توزيعة فيدورا ١٠

أعلن فريق تطوير فيدورا إطلاق النسخة الجديدة المنتظرة من العديدن من محبي هذه التوزيعة وهي الإصدار الذي يحمل الرقم ١٠ ضمن الإصدارات العديدة للمشروع.

وشهدت التوزيعة الجديدة العديد من التحديثات والإضافات الجديدة كمدير الحزم RPM بالإصدار 4.6 وتحسين عملية التعامل مع الطابعات المختلفة بالإضافة إلى العديد من البرامج الأخرى.
يمكن تحميل نسختك المجانية من خلال صفحة المشروع الموجودة من خلال الرابط التالي:

http://fedoraproject.org/en/get-fedora

الدليل السريعُ للإصدارِ الثالثِ من الرُّخصة المُشاعة العامة "GPL"

ترجمة وإعداد: بدري دركوش

مقدمة



بعد سنة ونصف من المناقشات والاستشارات العامة، وبعد آلاف التعليقات وأربع مسودات، صدرت أخيرًا النسخة الثالثة من رخصة جنو العمومية (GPLv3)، بتاريخ ٢٩ حزيران (يونيو) ٢٠٠٧. وبينما كان هناك الكثير من النقاش حول الرخصة منذ ظهور أول مسودة لها، لم يتكلم كثير من الناس عن المزايا التي تقدمها للمطور. وضعنا هذا الدليل لملء هذا الفراغ، وسوف نبدأ بتذكير سريع لكل من:

البرمجيات الحرة، وحقوقُ النسخ المرفوعة (١) (Copyleft)، وهدف رخصة جنو المُشاعة العامة (GPL)، وبعد ذلك سوف نستعرض التغييرات الأساسية لنرى كيف سوف تساعد هذه التغيرات في تقدم هذه الأهداف وتطوير المزايا.

مبادئ وأساسيات الرُّخصة المشاعة العامة

لا يجب على البرمجيات أن تقيد حرية المستخدم، وهنالك أربع حريات يجب أن يحصل عليها كل المستخدمين:

- حرية استخدام البرنامج لأي غرض كان.
- حرية مشاركة البرنامج مع الأصدقاء والجيران.
- حرية التعديل في البرنامج ليناسب حاجات المرء الخاصة.
- حرية مشاركة تعديلات المستخدم مع الآخرين.

عندما يحقق برنامج ما كل هذه الحريات للمستخدمين، حينئذٍ ندعوه برنامجًا حرًا (free software).
المطورون والمبرمجون الذين يكتبون البرامج يطلقونها تحت بنود الرخصة المُشاعة لجنو، عندما يقومون بذلك سوف تصبح برمجيات حرة، وسوف تبقى برمجيات حرة، مهما يكن من يعدل أو ينشر هذه البرمجيات، نحن ندعو ذلك حقوق النسخ المرفوعة(١) (Copyleft): أي أن البرمجيات لها حقوق نسخ (copyright) ولكن عوضًا عن استخدام هذه الحقوق لتقييد المستخدمين -كما تفعل البرمجيات المملوكة- نحن نستخدم هذه الحقوق لنتأكد أن كل المستخدمين يملكون الحرية.
لقد قمنا بتحديث الرخصة المُشاعة لحماية حقوق النسخ المرفوعة من التلاعب والتجاوز من قبل القانون أو التطورات التقنية. إن النسخة الأخيرة تحمي المستخدمين من ثلاثة تهديدات حديثة، وهي:

* تيفوزيشن(٢) (Tivoization): بعض الشركات التي صنّعت العديد من التجهيزات المختلفة والتي تستخدم برمجيات محمية برخصة جنو العامة، وبعد ذلك أعدت هذه التجهيزات لكي تقوم بتعديل البرمجيات التي تشغلها، لكن أنت لا تستطيع ذلك. إذا كان الجهاز يستطيع أن يشغل برمجيات تحكمية - على كمبيوتر متعدد الاستخدامات - والمالك يجب عليه أن يتحكم بما يقوم به الحاسوب، عندما يعترضه هذا الجهاز من القيام بذلك، هذا ما ندعوه بـ تيفوزيشن(٢) (tivoization).

* القوانين التي تحظر البرمجيات الحرة: التشريعات مثل قانون حقوق النسخ الرقمية الألفية(٣) (Digital Millennium Copyright) وتعليمات الاتّحاد الأوروبي لحقوق الملكية، تجعل من كتابة أو نشر البرمجيات التي تتجاوز حماية الحقوق الرقمية(٣) (DRM) جريمة. هذه القوانين يجب ألا تتداخل مع الحقوق التي تمنحك إياها الرخصة المُشاعة العامة (GPL).

* صفقات الامتياز المنحازة(٤): بدأت مايكروسُفت حديثًا بإخبار الناس بأنهم لن يقاضوا مستخدمي البرمجيات الحرة لانتهاكهم براءة الاختراع (الامتياز)، طالما يحصلون عليها - أي البرمجيات الحرة - من مزودين يقومون بالدفع لمايكروسُفت من أجل الامتياز. في النهاية، تحاول مايكروسُفت الحصول على عائدات مالية من استخدام البرمجيات الحرة، وهذا ما يتعارض مع حرية المستخدم. يجب أن لا تُساهم أي شركة في ذلك.

النسخة الثالثة تحمل المزيد من التحسينات لجعل الترخيص أسهل للاستخدام والفهم من قبل الجميع، ولكن بالرغم من كل تلك التعديلات فجي بي إل٣ ليست رخصة جديدة جذريًا، بل هي تطوير على النسخة السابقة. رغم أن العديد من النصوص قد تغيرت، أصبح الكثير منها يوضح ما قالته جي بي إل ٢ ببساطة. مع وضع ذلك بالاعتبار، لنرى التغيرات الأساسية في الإصدار الثالث ونتحدث عنه وكيف تحسنت الرخصة فيه بالنسبة للمستخدم والمطور.

تحييد القوانين التي تحظر البرمجيات الحرة، ولكن ليس حظر DRM

ربما تكون متآلفًا مع نظام إدارة الحقوق الرقمية(٥) (DRM) على الأقرص الرقمية والوسائط الأخرى، وربما أيضًا تكون معتادًا على القانون الذي يجعل من كتابة أدواتك الخاصة لتجاوز هذه القيود أمرًا غير قانونيّ، مثل قانون الحماية الرقمية الألفية(٣) وتعليمات الاتحاد الأوروبي لحقوق الملكية. يجب أن لا يمنعك أي أحد من كتابة أي شفرة تَريد كتابتها، الإصدار الثالث من الرخصة المُشاعة العامة يحمي هذا الحق لك.

يُمكن دائمًا كتابة شفرة محمية برخصة جي بي إل تحقق إدارة الحقوق الرقمية(٥)، ولكن إن قام أحدهم بذلك مع شفرة محمية برخصة جي بي إل ٣؛ يقول البند الثالث: أن النظام لن يعتبر ذلك مقياس حماية تقنيًا فعّالًا، وهذا يعني أنك إذا كسرت حماية(٥) الحقوق الرقمية فستكون حرًا في توزيع البرمجيات التي تقوم بذلك، ولن تكون مهددًا بقوانين مثل(٣) DMCA أو غيرها.

كالعادة.. رخصة جنو المُشاعة العامة لا تقيد ما يفعله الناس في برمجياتهم، ولكنها تمنعهم من تقييد الآخرين فقط.

حمايةُ حقوقكِ من المُدَّعين(٦)

تيفوزيشن (٢): هي محاولة خطيرة لاختزال حرية المستخدم، فحقك في تعديل البرمجيات سيصبح دون معنى إذا كانت أجهزة حاسوبك تمنعك من القيام بهذا.

الإصدار الثالث من جي بي إل يمنع التيفوزيشن(٢) عن طريق الفرض على الموزع بتزويدك بما تحتاجه من معلومات أو بيانات ضرورية لتثبيت البرمجيات المعدلة على الجهاز، والتي قد تكون ببساطة مجموعة من التعليمات أو التوجيهات، أو قد تتضمن بيانات خاصة مثل مفاتيح مشفرة (Cryptographic Keys)، أو معلومات حول تجاوز الفحص النظامي للجهاز. هذا يعتمد على طريقة تصميم هذا الجهاز، ولكن مهما كانت المعلومات التي تحتاجها يجب أن تستطيع الحصول عليها.

هذه الإمكانيات مازالت في هذا النطاق، ولا يزال يُسمع للموزعين بوضع مفاتيح مشفرة لأي غرض كان، وسيفرض عليهم كشف المفتاح فقط إذا أردت تعديل البرمجيات المحمية بالرخصة المُشاعة العامة على الجهاز الذي أعطوك إياه. مشروع جنو يستخدم GnuPG لتحسين التكاملية بين كل البرمجيات على موقعه لتبادل الملفات (FTP site)، ومقاييس كهذا يكون ذا منفعة للمستخدمين.

جي بي إل ٣ لا تمنع الناس من استخدام التشفير (لا نريدها أن تفعل ذلك) ولكنها تمنع الناس من أخذ ما أعطتهم إياه الرخصة بعيدًا، سواءً كان عن طريق الامتياز أو التقنية أو أي بند آخر.

حمايةٌ قوية ضدَّ تهديدات الامتياز (براءةُ الاختراعِ)

خلال سبع عشرة عامًا، ومنذ نشر الإصدار الثاني من الرُخصة المشاعة العامة، تغيرت رؤية امتيازات البرمجيات بشكل ملحوظ، وطَوّرت رخص البرمجيات الحرة استراتيجيات جديدة حتى تخاطبها. يعكس الإصدار الثالث من هذه الرخصة هذه التغييرات أيضًا.

كلما قام شخص بنقل برمجيات محمية برخصة جي بي إل ٣ (والتي كتبها أو عدّلها) يجب عليه أن يزود كل متلقّ لها -أي البرمجيات- أية رخصة امتياز ضرورية لاستعمال الحقوق التي تمنحها إياه الرخصة المُشاعة العامة، وامتيازهم سوف يصبح منّتهيًا.

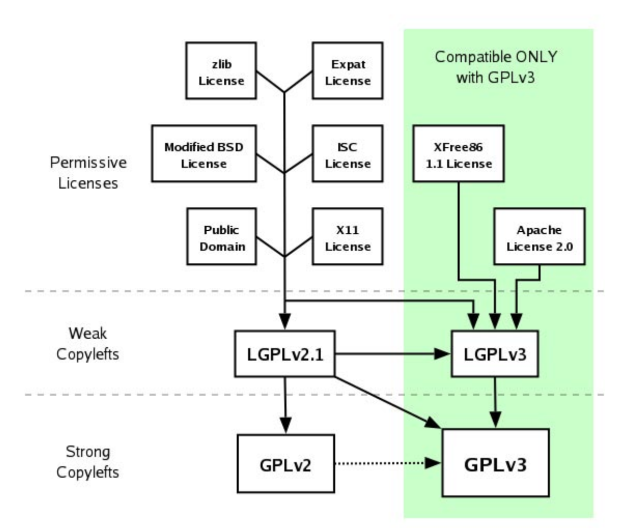
ذلك يعني للمستخدمين والمطورين أنهم سوف يتمكنون من العمل مع البرمجيات المحميّة برخصة جي بي إل ٣ دون القلق من مساهم يائس ما سيحاول محاكمتهم من أجل انتهاك الامتياز لاحقًا. مع هذه التغييرات.. جي بي إل ٣ توفر للمستخدمين المزيد من الدفاعات ضد تعديات الامتياز، أكثر من أي رخصة برمجيات حُرّة أخرى.

إيضاحُ الانسـجامِ بين التراخيص

إذا وجدت شفرةً ما وأردت دمجها مع مشروع محمي بالرخصة المُشاعة العامة؛ تقول رخصة "جي بي إل٢": يجب على الرخصة الأخرى ألا تحمل أية قيود موجودة سابقًا في رخصة جي بي إل ٢، وطالما حققت هذه القضية نقول أن الرخصة متوافقة مع رخصة جِنو المُشاعة العامة "جي بي إل".
على أي حال.. بعض الرخص كانت لديها متطلبات غير مُقيدة لأن الموافقة عليها كانت سهلة. على سبيل المثال: بعض الرخص تقول أنها لا تمنحك الحق باستخدام بعض العلامات التجارية المسَجلة (trademark) المحددة، وذلك لم يكن تقييدًا إضافيًا حقيقيًا. إذا كانت العبارة غير موجودة، فمازلت لا تملك الحق باستخدام العلامة التجارية المسجلة، ولا طالما قلنا أن هذه التراخيص متوافقة مع رخصة "جي بي إل٢" أيضًا.
الآن، الإصدار الثالثُ من الرُّخصة المُشاعة العامة يمنح بوضوح الحق للجميع باستخدام شفرة تستخدم متطلبات كهذه، وهذه البنود الجديدة يجب أن تساعد على إيضاح سوء الفهم حول الرخص المتوافقة مع رخصة جِنو المُشاعة. لماذا كل هذا وما الذي يمكن عمله مع شفرة متوافقة مع رخصة جِنو المُشاعة "جي بي إل".

الرخصُ الجديدةُ المتوافقةُ

لتوضيح القواعد حول الرخص المتوافقة مع رخصة جِنو المُشاعة السابقة، "جي بي إل ٣" أيضًا متوافقة معها مع بعض التراخيص الأخرى، ورخصة أباتشي (Apache License ٢,٠) هي مثال رئيسي. الكثير من البرمجيات الحرة العظيمة موجودة تحت هذه الرخصة مع وجود مجتمع قوي يحيط بها. نحن نأمل أن هذا التغيير في رخصة "جي بي إل ٣" سوف ينشئ المزيد من التعاون والمشاركة ضمن مجتمع البرمجيات الحرة، والشكل التالي يساعد على إيضاح بعض العلاقات المتوافقة بين التراخيص المختلفة للبرمجيات الحرة:



الأسهم التي تشير من ترخيص إلى آخر تدلّ على أن الترخيص الأول متوافق مع الترخيص الثاني، هذا صحيح إذا تبعت عدة أسهم لتصل من ترخيص إلى آخر. أي على سبيل المثال؛ رخصة ISC متوافقة مع "جي بي إل ٣"، وكذلك "جي بي إل ٢" متوافقة مع "جي بي إل ٣" إذا كان البرنامج يسمح بالاختيار لـ" أو أي إصدار أحدث" كما تنص رخصة جِنو المُشاعة، وهو ما يحصل في أغلب البرمجيات التي تطلق تحت هذه الرخصة "جي بي إل ٢". هذا الشكل غير شامل (انظر إلى صفحة الترخيص لدينا للحصول على لائحة كاملة للتراخيص المتوافقة مع "جي بي إل ٢" و"جي بي إل ٣")، ولكن يظهر بوضوح أن "جي بي إل ٣" متوافقة مع كل ما هو متوافق مع "جي بي إل ٢". وأكثر من ذلك أيضًا.
جِنو أفيرو (GNU Affero GPL version ٣): أصبحت جزءًا من التجمع، إن رخصة أفيرو جي بي إل الأصلية صممت لتضمن إمكانية الحصول على المصدر لكل مستخدمي تطبيق الوب. إذًا فجنو أفيرو جي بي إل توسع هذا الهدف: إنها قابلة للتطبيق على كل برمجيات الشبكة التفاعلية، لذلك سوف تعمل جيدًا من أجل برامج مثل خوادم الألعاب. التدبير الاحتياطي الإضافي أكثر مرونة أيضًا، وذلك إذا استخدم شخص ما مصدرًا محميًا بـ"AGPL" في تطبيق دون واجهة شبكية فسوف يتوجب عليه أن يوفر هذا المصدر بنفس الطريقة التي تتطلبها رخصة جنو العمومية. بجعل هاتين الرخصتين متوافقتين سوف يتمكن مطورو برمجيات الشبكة التفاعلية من تقوية حقوقهم للنسخ الحر (Copyleft) وبنفس الوقت يستطيعون البناء على المصدر القوي المحمي برخصة جِنو المُشاعة والمتوفر لديهم.

المزيدُ من الطرق للمطورين، للتزويد بالمصدر

أحد المتطلبات الرئيسية لرخصة جِنو المُشاعة أنك وعندما توزع شفرةً تنفيذيةً للمستخدمين، يجب عليك تزويدهم بطريقة للحصول على المصدر. رخصة جي بي إل٣ تعطيك بعض الطرق للقيام بذلك، وهي تحافظ على هذه الطرق مع بعض الإيضاحات وتقدم لك أيضًا طرقَ جديدةً للتزويد بالمصدر عندما تنقل الشفرة التنفيذية عبر الشبكة. على سبيل المثال، عندما تستضيف شفرة تنفيذية على خادوم ويب أو خادوم تبادل ملفات (FTP site) تستطيع ببساطة تزويد الزوار بكيفية الحصول على المصدر عن طريق خادوم طرف ثالث. بفضل هذا الخيار الجديد ستصبح تلبية هذا المطلب أسهل لكثير من الموزعين الصغار واللذين يقومون بتعديلات طفيفة فقط على البنية الكبيرة للمصدر.
الترخيص الجديد يجعل من السهل أيضًا نقل الشفرة التنفيذية عن طريق البِتُّورنت (BitTorrent)، بداية الأشخاص الذين ينزّلون أو ينشرون من التُّورنت معفيون من متطلبات الترخيص اللازم لنشر البرمجيات، عند ذلك أيًّا كان من يبدأ التورنت يستطيع التزويد بالمصدر عن طريق إخبار مستخدمي التورنت الآخرين عن توفره على خادوم شبكة عام، بكل بساطة.
هذه الخيارات الجديدة تساعد على إبقاء الرُخصة المُشاعة العامة في صف واحد مع معايير المجتمع الحر لتوفير المصدر من دون جعل ذلك صعبًا على المستخدمين في الحصول عليه.

توزيعٌ أقلُّ للمصدر: نظام مكتبات استثنائيٍّ جديد

كلا نسختي الرخصة المُشاعة العامة تتطلب توفير كل المصادر الضرورية لبناء البرمجيات، متضمنةً مكتبات الدعم ونصوص الإنشاء وما إلى ذلك، وقامت بحد (استثناء) مكتبات النظام: لست ملزمًا بتزويد المصدر لمكونات أساسية محددة من نظام التشغيل مثل مكتبة C.
جي بي إل ٣ حددت تعريف مكتبات النظام لتتضمن البرمجيات التي قد لا تأتي بشكل مباشر مع نظام التشغيل، ولكن كل مستخدمي البرمجية يتوقعون وجودها عندهم بشكل معقول. على سبيل المثال أصبح يتضمن الآن المكتبات القياسية للغات البرمجة المعروفة مثل بايثون وروبي.
بشكل واضح يجعلك التعريف الجديد تستطيع الجمع بين برمجيات محمية بالرخصة المُشاعة العامة مع مكتبات نظام رخصها متوافقة مع الرخصة المُشاعة العامة، مثل مكتبات C الخاصة بنظام أوبن سُلارس، وتوزيعهما معًا. هذه التغييرات ستجعل من حياة موزعي البرمجيات الحرة والذين يرغبون بتزويد المستخدمين بهذا التركيب أسهل.

ترخيصٌ عالميٌّ

تتحدث جي بي إل ٢ عن "التوزيع" (distribution) كثيرًا؛ عندما تشارك البرنامج مع شخص آخر، فأنت تقوم بتوزيعه. لم يتحدث الترخيص أبدًا عن ماهية التوزيع لأن المصطلح مستعارٌ من قانون الولايات المتحدة لحقوق النسخ، وقد توقعنا أن يبحث القضاة عن تعريفه هناك. من ناحية ثانية وجدنا أن قوانين حماية حقوق النسخ في البلدان الأخرى تستخدم نفس الكلمة، ولكنها تعطيها معنى آخر، وبسبب ذلك، فإن القاضي في مثل هذه البلاد قد يحلل جي بي إل ٢ بشكل مختلف عن القاضيِ في الولايات المتحدة.
الرُخصة المُشاعة العامة الثالثة تستخدم المصطلح الجديد "النّقل" (convey) وتوفر تعريفًا لهذا المصطلح يحمل المعنى نفسه الذي عنيناه بالتوزيع، ولكنه الآن مشروح بشكل مباشر ضمن الترخيص، ويجدر أن يكون المعنى سهل الفهم من قبل الناس أينما كانوا. هناك تعديلات صغيرة أخرى ضمن الترخيص تضمن تطبيقه بشكل متناغم على مستوى العالم أجمع.
عندما تتُجَاوز القواعد: سبيلٌ هادئ للمطاوعة(٧)
تحت ترخيص جي بي إل ٢؛ إذا قمت بالاعتداء على الترخيص بطريقة ما، فسوف تخسر حقوقك تلقائيًا وإلى الأبد. الطريقة الوحيدة لتحصل عليها مجددًا هي عن طريق الالتماس إلى صاحب حقوق النسخ، في حين يكون هناك دفاع جيد ضد الاعتداء. هذه السياسة قد تسبب الكثير من الإزعاج للشخص الذي يتورط مع القوانين عن طريق الخطأ.
الطلب من جميع أصحاب الحقوق تجديد الترخيص ربما يكون مرهقًا ومكلفًا أيضًا؛ توزيعة جنو/لينكس نموذجية مبنية على عمل الآلاف.
جي بي إل ٣ توفر تخفيفًا من أجل التصرف الجيد: إذا قمت بانتهاك الترخيص سوف تستعيد حقوقك حالما توقف الانتهاك إلا إذا اتصل بك صاحب حقوق النسخ خلال ٦٠ يومًا. بعد أن تتلقى ملاحظة من هذا النوع، سوف تستعيد حقوقك كاملة إذا كانت هذه أول مرة تقوم بانتهاك وقمت بإصلاح الانتهاك خلال ٣٠ يومًا. وإلا فسوف تعمل على المسألة قضية-قضية على حسب مالك حقوق النسخ الذي ...

... الذي اتصل بك، وسوف تستعيد حقوقك بعد ذلك.

لطالما كانت المطاوعة(٧) مع رخصة جنو المُشاعة أولوية بالنسبة لـ(FSF Compliance Lab) ومجموعات أخرى تنفذ الترخيص على نطاق العالم. هذه التغيرات تضمن أن المطاوعة(٧) تبقى أولوية عليا للمنفذين وتعطي المنتهكين حافزًا لكي يستجيبوا.

أخيرًا والأهمُّ

يُحتمل أن تبدو بعض هذه التغييرات أقل أهمية لك عن الآخرين، ولا بأس بذلك، فكل مشروع مختلف، وله احتياجات مختلفة من الترخيص، ولكن الأفضلية تكمن بأن عددًا من هذه التحسينات سوف تساعدك وتسهل عملك.
وعندما نأخذ بالمجمل، فكل هذه التحديثات تقدم شيئًا أكثر: لقد صنعنا حقوق نسخ حرة أفضل (Copyleft). إنها تقوم بالمزيد من أجل حماية حرية المستخدمين، ولكن أيضًا تمكن المزيد من التعاون ضمن مجتمع البرمجيات الحرة. تحديث الترخيص هو جزء من العمل: لكي يحصل الناس على المزايا التي توفرها، يحتاج المطورون لاستخدام جي بي إل ٣ لمشاريعهم أيضًا. عندما تطلق مشروعك الخاص تحت الترخيص الجديد، فكل من يتعامل معه -من مستخدمين أو مطورين آخرين أو موزعين أو حتى محامين- سوف ينتفع. نأمل أن تستخدم جي بي إل ٣ لإصدارك التالي .
إذا أردت أن تعلم المزيد حول تحديث مشروعك إلى الرُّخصة المُشاعة العامة الثالثة، فسوف يكون FSF Compliance Lab سعيدًا ليساعدك. على موقعهم، تستطيع الحصول على التعليمات الأساسية لاستخدام الترخيص.

الهامش من المترجم:

(١) copyleft = حقوق النسخ المرفوعة.
(٢) Tivoization = تيفوزيشن لم أجد أي ترجمة لهذا المصطلح حتى باللغة الإنكليزية، لذلك هو يشرح نفسه .
(٣) Digital Millennium Copyright Act هو قانون في الولايات المتحدة الأمريكية لمنع نسخ وتعديل المنتجات الرقمية.
(٤) المصطلح الأصلي للتوضيح Discriminatory patent deals.
(٥) Digital Restrictions Management = إدارة الحقوق الرقمية.
(٦) Tinker = المدعين.
(٧) Compliance = المطاوعة.

- كلمة المصدر الواردة في الترجمة تعني الشفرة المصدرية (source code) للبرنامج.
أرجو إعلامي عن أي ملاحظات أو نصائح خاصة بهذه الترجمة بمراسلتي على:
free-programmer@linuxac.org

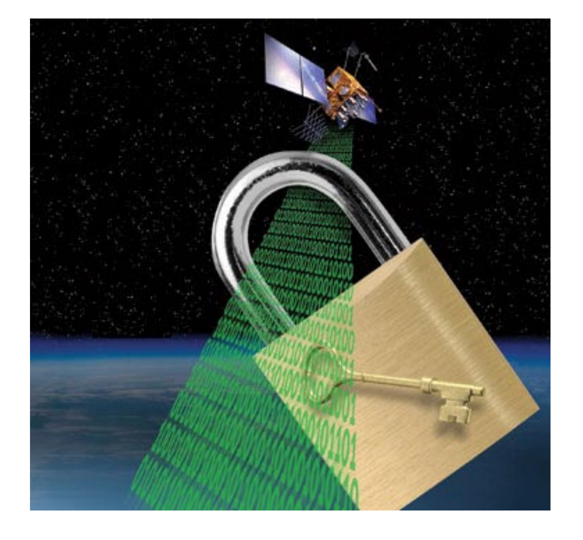
الكاتب الأصلي:Brett Smith
Free Software Foundation, Inc.
licensing@fsf.org

Free Software Foundation, Inc.
licensing@fsf.org

تشفير البيانات القياسي Data Encryption Standard (DES)

إعداد: صبري صالح

مقدمة



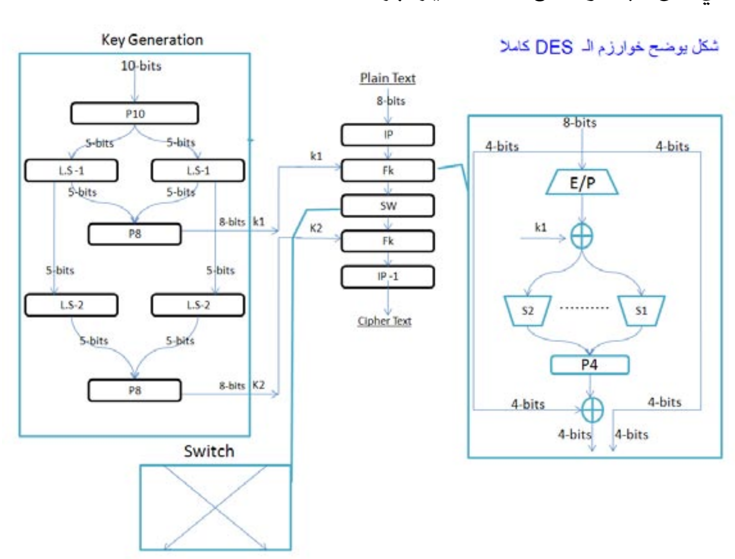
موضوعنا اليوم لن أقول بأنه جديد، لكني أكاد أجزم بأنه لأول مرة يتم عرضه بهذه الطريقة بين الصفحات العربية. لن أعرّف هنا معنى كلمة تشفير؛ لأن المقدمة الواجب أن أضعها قد وضعها إخواني في المنتديات وجزاهم الله عنا خير الجزاء. لكني سأضع أمامك مادة علمية قوية جدا تشرح واحدا من أقدم خوارزميات التشفير وأقواها -قد يعترض أكثركم على كلمة أقواها، لكن عندما تم عمل هذا الخوارزم و اعتماده كان من أقوى أنواع التشفير في و قته، وقد تم تحديثه أكثر من مرة وأصبح هناك: Double DES و Triple DES و Advanced DES-.

في نهاية الموضوع سيتضح لنا معنى كلمة تشفير وكيف يتطور علم التشفير بالنسبة للتشفير المتماثل Symmetric Encryption وما سيأتي في السطور التالية لن يكون غريبا عنك.

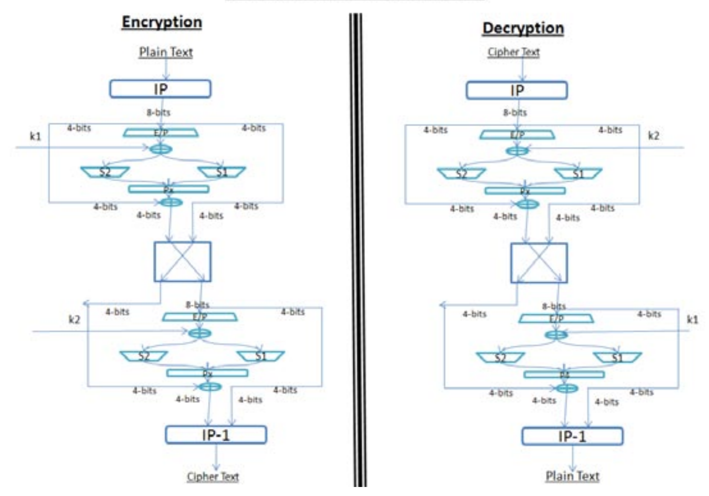
Data Encryption Standard (DES)

تم اختياره عام ١٩٧٧م من قبل المعهد الدُولي للمعايير التكنولوجية National Institute of Standard Technology أو NIST على أنه معيار دُولي للتشفير، ويتم على أساسه التطوير في أنواع التشفير التي هي من فئته أي Symmetric Encryption، وقد كان لـ IBM باع في وضع بذرة هذا التشفير لا نستطيع تجاهله.

ملاحظة: هذا العلم درسته في آخر سنة لي في هندسة الحاسب الآلي و طرحه يجبرني على الاعتماد على أن قارئ الموضوع يعرف أساسيات التعامل مع نظام الترقيم الثنائي Binary Number System ومع العمليات المنطقية، وقد نوّهنا إلى أن أساسيات التشفير والمقدمة المطلوبة قد كتبها إخواني من قبل و Google خير برهان.



شكل يوضح خوارزم الـ DES كاملا



ربما لم نتمكن من فهم الرسومات السابقة، لكن سنحاول فهمها في الأسطر التالية وفي الغالب فإننا سنعرف الأشياء بمعناها العلمي؛ أي نعرفها بوظيفتها لنبتعد عن الكلام النظري البحت.
يجب أن نضع دومًا في الحسبان أنّ تعاملنا مع البيانات Data سيكون بالترقيم الثنائي، وفي بعض الأجزاء سنستخدم نظام الترقيم العشري Decimal Number System.

تعاريف

Initial Permutation أو IP

نقصد بها "اللخبطة"، والترجمة الحرفية لها: "التبديل المبدئي". وظيفتها هي أن ندخل لها ٨ بت فتقوم بتغيير أماكنهم بشكل غير مُنظّم بناءً على أرقام تم تحديدها بطلبنا و تكون من رقم ١ إلى رقم ٨، لكن تلك الأرقام غير مرتبة... حسنًا، لنجرب مثالا عمليًا حتى نفهمها.

لدينا ٨ bits وهم من اليسار إلى اليمين كالتالي: 10011101
إذًا ترتيب أول bit الذي هو ١ سيكون ١، والثاني الذي هو ٠ سيكون ٢، إلخ....

لذلك إذا كان عندنا: IP = 26314857 وتقرأ أيضًا من اليسار إلى اليمين؛ فهو يقصد أن يلخبط أول Bit عندنا الذي هو ١ ويجعله الثاني وترتيب ثاني Bit عندنا الذي هو ٠ سيكون السادس، و هكذا.

أي أن ال Stream السابق (10011101) سيصبح بعد إدخاله في عملية ال Initial Permutation هكذا (01011110).

مثال آخر :

Data = 10011101

[IP= [26314857

Data(IP) = 11010110

الترتيب الطبيعي لـ bits	1 2 3 4 5 6 7 8
Data	1 0 0 1 1 0 1 1
Initial Permutation	2 6 3 1 4 8 5 7
Data After Permutation	1 1 0 1 1 1 1 0

Inverse Initial Permutation أو IIP

نرقم ال Inverse Initial بالترتيب من اليسار إلى اليمين
ننظر إلى أرقام الترتيب الطبيعي لل Bits ثم نجعل ترتيبها في المكان الذي يساوي الرقم المقابل له في ال Initial Inverse

وبهذا نكون قد أخرجنا أرقام الترتيب العكسي.

أرقام Initial Permutation	2 6 3 1 4 8 5 7
الترتيب الطبيعي لـ bits	1 2 3 4 5 6 7 8
ارقام Inverse Initial Permutation التبديل العكسي	4 1 3 5 7 2 8 6
Data After Permutation	1 1 0 1 1 1 1 0
Data After Inverse Permutation (Original Data)	1 1 0 1 1 0 1 1

Expansion Permutation أو E/P

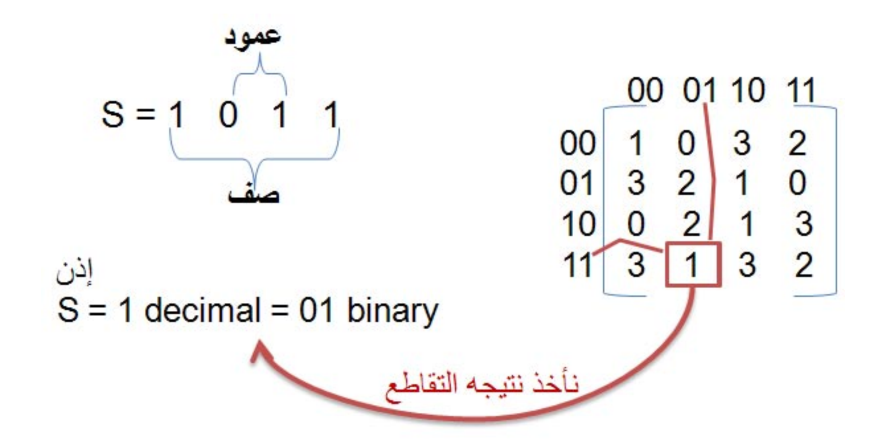
هي عملية اللخبطة أيضًا كما عهدناها، لكن ستتسبب في زيادة عدد ال bits؛ لذلك سُميت Expansion، و طريقتها هي تكرار ال bit على حسب تكرار مكانه في ال E/P

مثال عملي:

ارقام Expansion Permutation (E/P)	4 1 2 3 2 3 4 1
	1 1 0 0
Data After Expansion Permutation	0 1 1 0 1 0 0 1

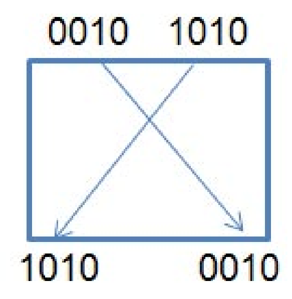
S-Box

هي عملية Permutation لكنها مختلفة تمامًا عن سابقاتها، وتتسبب في تقليص عدد ال bits إلى ٢bits، وتستخدم التبديل بالمصفوفات Matrices لإيجاد قيمتها، وفي المسائل العملية فإنك تعطى المصفوفة القيمة S التي ستخرجها من تقاطع الصف مع العمود ثم تحول القيمة إلى النظام الثنائي Binary System.



SW أو Switch

عملها يتضح من اسمها؛ فهي تقوم باستبدال مسار ال bits التي في ناحية إلى الناحية الأخرى.



Key Generator

هو مولد المفاتيح التي ستضاف إلى البيانات لتزداد عملية اللخبطة أو تعقيد التمويه والتبديل، ونستطيع أن نولد أكثر من مفتاح فرعي Sub key في ال DES.

Lift Shift

يعني ترحيل أو إزاحة عدد محدد يتم تحديده. بدايةً، نزيح الأول بمقدار واحد والثاني بمقدار ٢، وهكذا -يجب أن تراقب الرسمة الأساسية أيضًا لتكتمل مُخيّلتك العلمية-، ويقوم بإزاحة ال bits من اليسار إلى اليمين بغرض اللخبطة، ويستقبل في ال DES عدد 5-bits، وعندما تحدد عدد الإزاحات فإنه يبدأ بالإزاحة من اليسار إلى اليمين، ويرمز أيضًا لها بهذه العلامة "<<<".

سنفهم بمثال خفيف:

k1 k2 k3 k4 k5

نريد أن نعمل لهم إزاحة بمقدار ٣ من اليسار إلى اليمين؛ فالناتج سيكون:

k4 k5 k1 k2 k3

حيث إن k تعبر عن ال bit الواحد.

XOR

هي عملية منطقية يكون ناتج ال bits المتشابهة فيها ٠ والمختلفة ١.

مثال :

```
  0 0 0 1 1 0 1 1
  0 1 0 0 1 1 1 1 ⊕
  ---------------
  0 1 0 1 0 1 0 0
```

حسنًا، سنتكلم مرةً أخرى عن الأجزاء التي عرفناها من التعاريف السابقة، لكن سنتكلم عنها من ناحية عملها ومهمتها في نظام التشفير هذا؛ فهذه الأجزاء ليست حصريةً لهذا التشفير ولكن يختلف تشفيرٌ عن آخر في شكل و خطة الخوارزميات وفي Block size of data وفي عدد تكرار الشيء وطريقة ترابط أجزاء البيانات Data المقسمة.
كل هذا الكلام عام، لنبدأ إذًا، وستفهم هذا المعنى عندما نشرح أكثر من نوع تشفير إن شاء الله.

١.حجم البيانات المراد تشفيرها Plain text block size

وُجِد أن أنسب حجم للبيانات المراد تشفيرها بالنسبه لـ DES هو ٦٤-bit وإن زادت حجم البيانات عن ذلك فإنها تُقسم كما يحدث في القرص الصُلب Hard Disk. لكن، لو كان حجم البيانات المراد تقسيمها لا يقبل القسمة على ٦٤؛ فإنه لكي نقسمها سنبحث عن آخر bit ثم نقوم بعملية ال Padding.
حسنًا، لنوضح هذا الأمر.

لنفرض أن حجم البيانات المراد تشفيرها هو 660-bit .
٦٦٠/٦٤=١٠,٣ ونحن نعلم أنه لا يمكن حجز جزء من ال Block of data ونترك الباقي فارغًا فيجب إما ملؤه أصفارًا، وهذا لا يصح مع التشفير لأنه سيأثر على شكل البيانات أصلا، أو أن هناك حلا آخرًا. بدون تفصيل هو:
أن نُقرب الرقم ١٠ حتى يصبح ناتج القسمة عددًا صحيحًا بدون كسور.
وهذا كلامٌ عامٌ بالنسبة لل padding، لكنه ليس موضوعنا أساسًا.

٢.المفتاح السري Secrete Key Size

تمامًا مثل مفتاح المنزل: به تُشفر البيانات وبه يُفك تشفيرها، وتجده على كل كلمة مرور في البرامج، وحجمه في ال DES يصل إلى 65-bit=8 characters.

٣.عدد اللفات Number of Rounds

عدد اللفات في المفاتيح ,DES=16-rounds=16-sub وكل Sub Key حجمه ٦٤-bit.

٤.توليد المفاتيح Key Generation

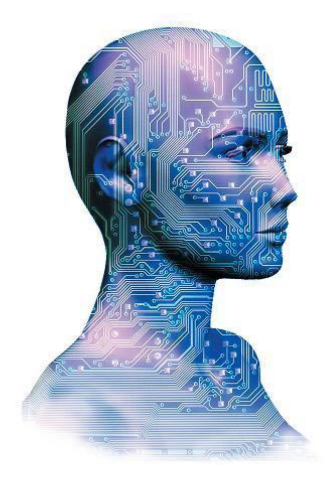
مولد المفاتيح هو الذي يخرج المفتاح الفرعي Sub key؛ فنحن نختار ال Secret key أما الـ Sub key فيكون عبارة عن ١٦×٤٨ حيث ٤٨ هو الحجم الأقصى للبت، وال ١٦ أقصى عدد للمفاتيح الفرعية يتحمله ال DES.
هذا الموضوع يحتاج إلى انتباه وإلى قراءته أكثر من مرة وذلك قبل أن أفكر في السؤال عن كسر تشفير ال DES رياضيًا بطريقة الاحتمالات أو بال Brute Force.

ملخص لأهم خصائص DES:

Characteristics	DES
Plaintext Block Size	64-bit
Key Size	56-bit
No. of Sub key	16-bit
Sub key Size	48-bit
No. of S-box	8-bit
S-box Size	4 ×16 -bit
No. of rounds	16-bit

معالجة الصور الرقمية

إعداد : يونس بوطيور



مقدمة

تعتبر معالجة الصور مجالا علميًا مرتبطًا بالرياضيات التطبيقية وعلم الحاسوب، و هي تدرس الصور الرقمية وكذا مختلف التحويلات والتعديلات الممكن تطبيقها عليها؛ وذلك بهدف الحصول على جودة أفضل أو من أجل استخراج معلومات من الصورة لاستغلالها من طرف الآلة أو الإنسان.

فهم ماهية معالجة الصور يبدأ من فهمنا للصورة نفسها ومكوناتها و خصائصها؛ فدعونا نرى تعريفًا مبسطًا لها.

١.عموميات

تعريف الصورة

الصورة هي تمثيل لشخص أو شيء بالصباغة، الرسم، النقش، آلة التصور، الفيديو، ...إلخ. وهي أيضًا أيضا مجموعة منظمة من المعلومات تخضع لدالة I(x,y) ذات لمعان متصل غير رقمي، مُعرّفة في مجال محدود، بحيث x و y هما إحداثيات لنقطة M من الصورة و "I" دالة لشدة الإضاءة و اللون.
لكن بهذه الخصائص يصعب استغلالها رقميًا مما يستدعي تحويلها إلى صورة رقمية.

تعريف الصورة الرقمية

هي كل رسم، أيقونة أو صورة استقبلت أو أنشات أو خُزنت على هيئة رقمية (0 و 1):
- استحصلت بواسطة المحولات الرقمية، و لتي تتواجد بالكاميرات الرقمية أو الماسح الضوئي أو غيرها من الأجهزة
- أنشأت أو عدلت على الحاسوب بواسطة البرامج المتخصصة في معالجة الصور كـ Gimp أو Paint أو Photoshop أو Blender وغيرها، وذلك بغرض إضافة أو حذف أو تغيير عناصر في الصورة
- خزنت على وحدة تخزين معلوماتية من قرص صلب أو مرن أو غيرها

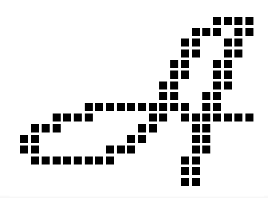
فالصورة الرقمية هي كذلك الصورة الممثلة بمصفوفة ثنائية الأبعاد f(x,y)، بحيث x و y هما إحداثيات نقطة من الصورة و f(x,y) قيمة اللون في هذه النقطة.

خصائص الصورة الرقمية

للصورة الرقمية مجموعة من الخصائص نذكر منها:

١.البيكسل:

وهو أصغر نقطة في الصورة. له تركيبة معينة ليمثل حاليًا أصغر عنصر يمكن للعتاد وللبرامج التعامل معه. مثال: يمكن تمثيل الحرف A على شكل مجموعة من البيكسيلات، صورة توضيحية:



كمية المعلومات الممثلة لكل بيكسل تفرق بين الصورة ذات تدرج اللون الرمادي و الصور بالألوان؛إذ بالنسبة للصور ذوات التدرج الرمادي فإن كل بيكسل يمثل على ثماني واحد octet، بينما للصور الملونة؛ فإن كل بيكسل يأخذ على الأقل ثلاث ثمانيات (3octets)، ثماني لكل لون في النموذج أحمر-أخضر-أزرق (RGB).

٢. الدقة:

وتعبر عن مدى جودة ووضوح التفاصيل بالنسبة لشاشة أو طابعة منتجة للصور، وهي عدد البيكسيلات في و حدة للقياس (Inch أو Centimeter). كما يمكن أن ترمز للعدد الإجمالي للبيكسيلات الأفقية والعمودية الظاهرة على الشاشة، كلما كانت أكثر كانت الدقة أعلى.

٣. الضجيج:

وهو ظاهرة تغير مفاجئ لشدة بيكسل بالمقارنة مع جيرانه.

٤.مخطط الألوان Histogram:

مخطط الألوان بالنسبة للصورة هو دالة تكشف لنا تردد ظهور الألوان في الصورة.

٥.الحواف:

هي الحدود بين العناصر المكونة للصور أو ذلك التغير البارز في شدة اللون بين بيكسيلين متجاورين.

٦.الإضاءة:

هي شدة إضاءة بيكسيلات الصورة.

٧.التباين:

هو ذلك الفرق بين شدة إضاءة منطقتين من الصورة إحداهما داكنة والأخرى مضيئة.



صورة رقمية بتقنية HDR

٢.عمليات أساسية على الصور الرقمية

الدوال المنطقية

تعتبر الدوال المنطقية من أبسط العمليات التي يمكن القيام بها على الصور الرقمية.

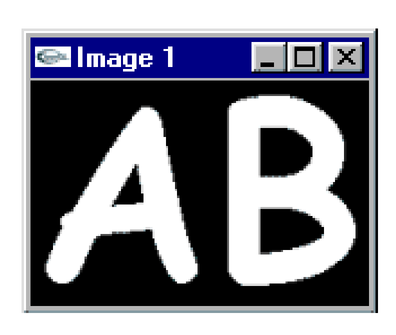
الدالة AND، ونرمز لها بالرمز &

و هي الدالة التي تجمع عنصرين من صورتين p1 و p2 للحصول على صورة ثالثة p تكون هي النتيجة.

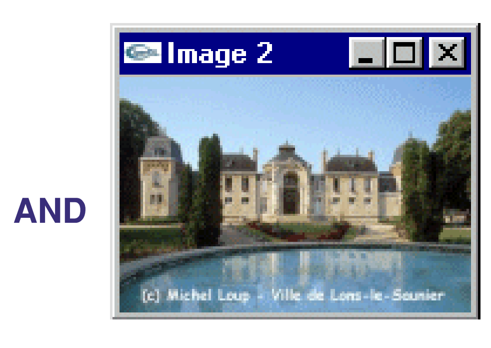
$$p(x,y) = p1(x,y) \& p2(x,y)$$

و هذا جدول حقيقتها:

AND	0	1
0	0	0
1	0	1



AND



=



الدالة OR، ونرمز لها بالرمز |

و هي الدالة التي تعطينا نتيجة طرح عنصرين من صورتين p1 و p2 للحصول على صورة ثالثة p تكون هي النتيجة.

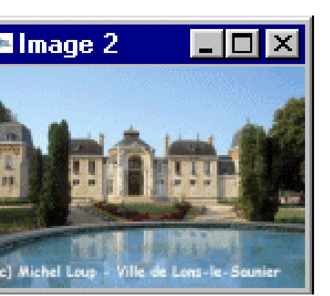
p(x,y) = p1(x,y) | p2(x,y)

و هذا جدول حقيقتها:

Or	0	1
0	0	1
1	1	1



AND

=



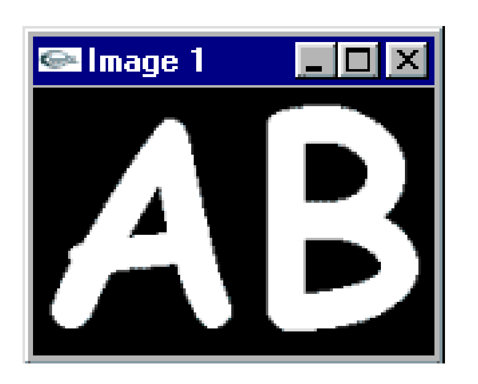
الدالة NOT، ونرمز لها بالرمز ~

و هي الدالة التي تعطينا نتيجة عكس عنصر من صورةp1 للحصول على صورة p تكون هي النتيجة.

$(p(x,y) = \sim p1(x,y)$

و هذا جدول حقيقتها:

Not	-
0	1
1	0



NOT



هذه فقط بعض الدوال المنطقية التي سنستخدمها في مقالات قادمة إن شاء الله.

خاتمة

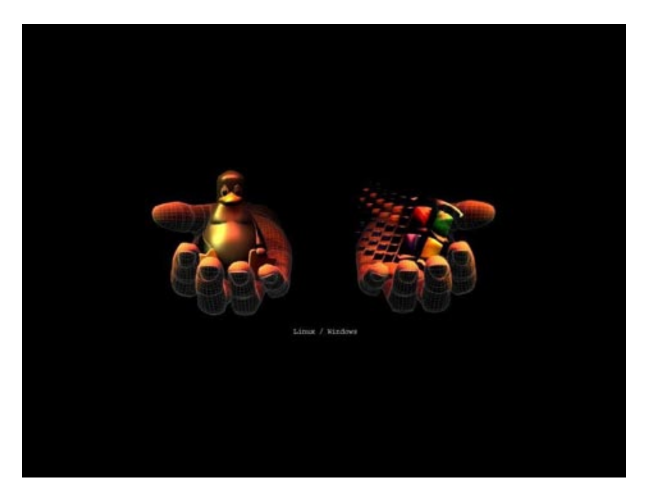
في هذا المقال تعرفنا على بعض المصطلحات والعمليات البسيطة في مجال معالجة الصور آملين أن تكونوا قد استفدتم ولنا لقاء في مقال آخر لإتمام رحلتنا مع هذا المجال الشيق.

المراجع :

http://fr.wikipedia.org/wiki/Traitement_d'image
http://raphaello.univ-fcomte.fr
http://xphilipp.developpez.com

القول الحاذق في تثبيت لينكس والمحافظة على النظام السابق

إعداد : أحمد السيد محمود



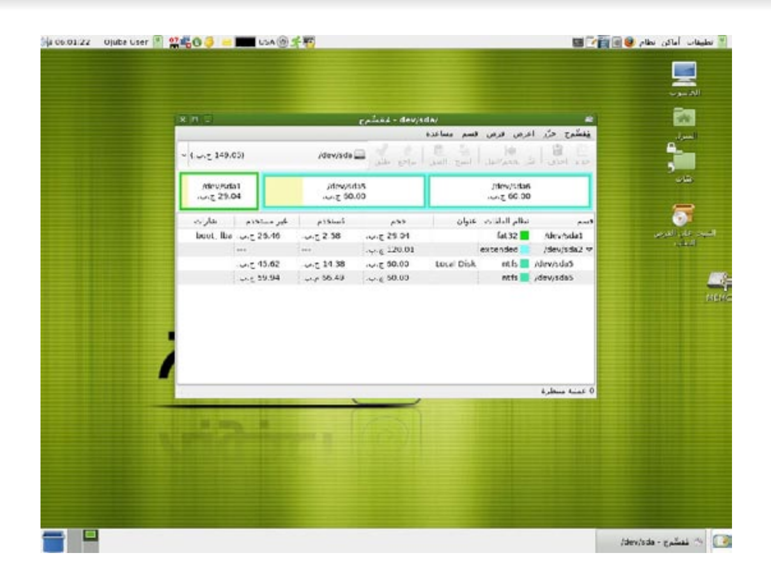
يعتبر تثبيت لينكس من أهم الموضوعات -إن لم يكن أهمها على الإطلاق-؛ وذلك لأن التثبيت هو بوابة التعرف على النظام وهو عنوان الكتاب، فإن نجح فما بعده أيسر وإن فشل فقد فشلت بداية التعرف على النظام أو التوزيعة، وهو ما يضر بشدة خصوصاً إذا كانت هناك توزيعات وليدة وواعدة. ولكن البعض لا يعرف كيف يثبتها ويتعامل معها ومن ثم يبدأ في كيفية التعلم.

معظمنا كانت له تجارب غير محبوبة مع التثبيت خصوصاً في التوزيعات التي تبدو للوهلة الأولى أنها صعبة، ولكن ما سبب ذلك؟ أغلب الظن أن جميع التوزيعات صعوبتها نسبية، فجميعنا يذكر كيف كان وندُز صعب التنزيل، وكيف كنا نحمل بيانات الجهاز في يوم كامل، وكانت المساحات والمواصفات في عصور ما قبل التاريخ، وكانت أيدينا ترتعش خوفاً من فقدان شيء أو حصول خطأ ما لا نعرفه، ونحن معذورون؛ فالإنسان عدو ما يجهل.
كلنا نعرف ذلك وكان لابد من هذه المقدمة لأن بعض الناس يحكمون على لينكس لمجرد أنهم فشلوا في تثبيته، أو لأنهم فقدوا بياناتهم عند تثبيته، ولكنني أؤكد أن كل ذلك ما هو إلا محض استعجال وضغط على الزر دون التثبت من محتواه وما يقول لنا، وحينها لا تلوموا إلا أنفسكم، فهل نزل النظام لوحده وبمفرده أم أن هناك أزراراً ضغطناها بأنفسنا، وهل راعينا وراقبنا ما تقول لنا هذه الأزرار أم أننا نضغط "موافق" أو زر "التالي" دون أن نكلف أنفسنا عناء الفهم!!
سأخبركم الآن بسهولة تنزيل لينكس من القرص الحي (Live CD)، النسخة الأولى من نظام التشغيل الرائع (أعجوبة)، وهذا كل ما نحتاجه فقط، لا برامج أخرى ولا أي شيء آخر. وسوف نحافظ على البيانات التي في حوزتنا، وليس هذا فقط بل سنبقي النظام السابق أيضاً، وكل ذلك في خطوات قليلة لا تتطلب سوى بضع دقائق فقط.. والآن، هيا بنا!

أولا: نضع القرص الحي في محرك الأقراص المدمجة (إذا لم تكن تملكه، فيمكنك الحصول عليه من مجتمع لينكس العربي، أو من موقع أعجوبة (Ojuba.org). سنختار الإقلاع من محرك الأقراص ونقلع. سيظهر أمامنا عدّاد، نترك القرص يقلع إلى حين الدخول ولا نفعل أي شيء، أو نختار الأول إذا تسارعت أيدينا بضغط زر الإدخال، وهو (Boot) سنلاحظ أن الدخول تلقائي، بعد ذلك سترى واجهة النظام. ربما تلاحظ بطئاً في النظام إذا لم تكن مساحة ذاكرة جهازك على الأقل ٥١٢ ميغابايت، فلا تنزعج وحدث جهازك!

ثانيا: نختار من الأعلى "تطبيقات" ثم "أدوات النظام"، ثم نختار برنامج تحرير الأقسام (G parted partition Editor) -كما في الصورة التالية:





ستظهر واجهة البرنامج -كما في الصورة أعلاه-، وسنلاحظ صورة وبيانات أولية لمعظم الأقراص التي نستخدمها، وهنا بصورة مبسطة سنلاحظ أول قسم من أقسام القرص الصلب وهو (Sda1)؛ وهذا هو (:C) أو أول قسم في أي نظام شائع، وسنلاحظ اللون الأخضر وأمامه مكتوب (Fat32)؛ وهذا هو الشائع والمعروف من أيام "ويندوز ٩٨" حيث كان قبلها نظام ملفات (Fat16) الأقدم.

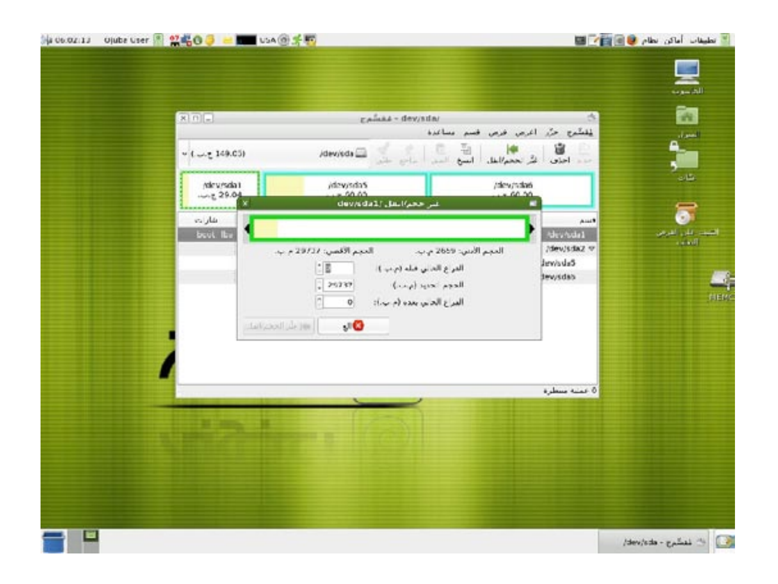
(ملاحظة مهمة: تستطيع الاستزادة عن أنواع أنظمة الملفات، وكيفية تهيئتها (فورمات) من المواقع التعليمية -إذا كنت تجهل ذلك-؛ ومنها مجتمع لينكس العربي). فقط ينبغي أن تعرف أن أنظمة (FAT) و (NTFS) مقروءة في لينكس، على عكس وندُز الذي لا يقرأ أنظمة ملفات غيره مثل (Ext3)، وهي أنظمة ملفات لينكس الشهيرة، أو مساحة التبديل (السواب)؛ وهي نظام ملفات للذاكرة الوهمية التي يستخدمها النظام من القرص الصلب. إن هذا كله لا يتطلب منك -إذا لم تكن محترفاً- أن تتدخل يدويا، تستطيع فقط اختيار التثبيت التلقائي. (سنعرف لاحقاً) .

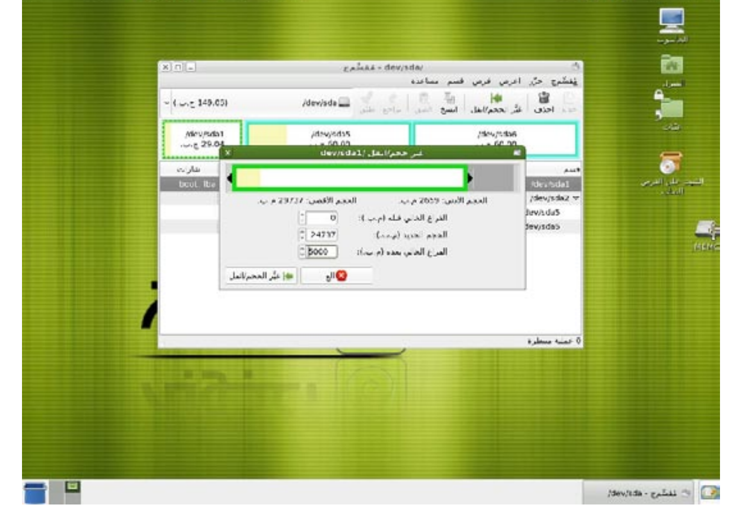
ستلاحظ أيضا في الصورة السابقة أن نوع أول قسم "رئيسي" (Primary)، وتظهر بعد ذلك معلومات عن القرص الموسّع (Extended)؛ وهو ينقسم إلى قسمين "منطقيين" (Logical) نظام ملفات كل منهما NTFS، وهذا كله إذا كان القرص MSDOS = Table.
(قد لا تتماثل معظم الأقراص مع هذا التقسيم بالضبط، ولكني أطرح ما يمكن فهمه وتطبيقه مع القياس على ما أقوم به وأوضحه هنا، فقد يكون لدى البعض أكثر من قسم رئيسي كما قد يكون هناك أكثر من قسم منطقي، وقد لا تكون بالضرورة أنظمة ملفاتها NTFS فهذا غير مهم).

المهم هو أي قسم سنختار وأين سنثبت لينكس (ليس ضرورياً أن تثبته على أول قسم، يمكنك أن تختار ما يناسبك)، وسأختار هنا القسم الأول لكي أقول لبعضهم أن لينكس ينزل جنباً إلى جنب مع أي نظام آخر أو قد لا تكون هناك مساحات متوفرة غير هذا القسم. وسنفترض أن القسم الأول FAT32 وينزل عليه نظام إكس بي مثلاً أو فستا بنظام NTFS، غير مهم كل ذلك فمعنا البرنامج السحري المهم، نختار القسم ونضغط "غير الحجم" في الأعلى (إذا لم تكن نشطة (ولا يفترض حدوث هذا) فاضغط بزر الفأرة الأيمن على القسم المراد -والذي نعمل عليه- ثم اختر "أزل الضم").

انظر للصورة التالية (في الصفحة القادمة) ، سترى نافذة صغيرة في المنتصف تسرد لنا بيانات ومعلومات عن القسم الذي اخترناه للتو. المعلومة "الحجم الأدنى" تريك الحد الأدنى الذي يمكن أن نقسم الجزء المختار عليه، وهو يختلف باختلاف البيانات الموجودة على القسم؛ وذلك حتى لا تضيع البيانات، فإن كانت البيانات غير مهمة فلا حاجة لتغيير الحجم، ويمكنك أن تعيد تقسيم وتهيئة الجزء كما تشاء ثم تغير الحجم كما تريد!

اللون الأخضر المستطيل في اللقطة هو القسم المُختار، والأصفر هي البيانات الموجودة فيه.
البيان "الفراغ الخالي قبله" كل زيادة فيه ستنقص من القسم، وهنا نحدد عدداً مناسباً من الميغابايات بالأرقام (معروف أن كل ١٠٢٤ ميغا = غيغا واحدٌ) لتثبيت النظام فيه.



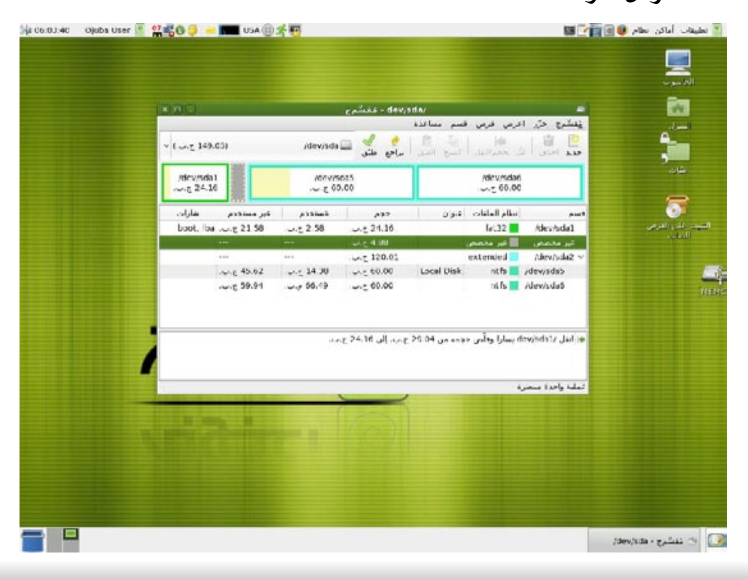


ولكننا سنترك الفراغ "قبله" هذا ونضغط على الزر لزيادة الميغابايتات في "الفراغ الخالي بعده"، والفرق بين الاثنين أن الفراغ "قبله" سيُنشئ لنا قسماً قبل السي (C)، ونحن نريد قسماً بعده؛ لكي نجعل النظام السابق أول قسم، فلا يتصرف بغرابة أو يتعطل إقلاعه، وهذا لأن الأنظمة الأخرى تتطلب وجود أول قسم نشط عليه ملفات معينة، وهذا جمود ليس كمرونة لينكس.

سنزيد في المربع الذي يقول "الفراغ الخالي بعده" أو قد نسحب جزءاً من الضلع الأيمن من المستطيل الأخضر إلى اليسار قليلاً، ولكن برفق، فكل ملم يعني زيادة شيءٍ من المساحة المطلوبة إذا استمر الضغط والسحب .

سنختار حجماً مناسباً -ويفضل أكثر من ١ غيغا- ثم نضغط "غيّر الحجم" بجوار زر الإلغاء - شاهد اللقطة إلى اليسار- .

في الصورة أدناه، سنرى بوضوح القسم الخالي الذي أنشأناه معنوناً بـ"غير مخصص"، وسنلاحظ أنه في الأسفل مكتوب (عملية واحدة منتظرة) وزر "طبِّق" في الأعلى نشط، وهذا معناه أننا يمكننا التراجع عن كل ذلك والبدء من جديد إذا ظهر لنا أي خطأ أو لاحت لنا فجأة خطط أخرى للتقسيم والتهيئة، فما زال الوقت لنا متسعاً.

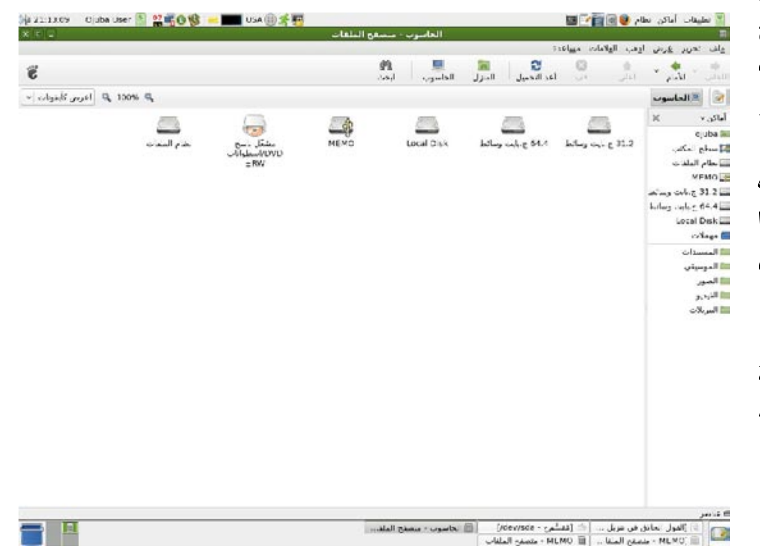




في اللقطة إلى اليمين، سنكون قد قررنا وعزمنا على المضي في التقسيم ونتوكل على الله ونضغط في الأعلى "طبق" (ستظهر رسالة تأكيد، لا تخف واضغط "طبق" تحت بجوار الإلغاء).
إذا أردنا أن نقسم أي قسم جزأين نتبع نفس الطريقة بزيادة الحجم وتغييره سنحصل على قسم متاح، والضم أيضاً يكون بنفس الطريقة ولكن بزيادة القسم المطلوب على حساب الجزء الفارغ.
إلى هنا نكون قد انتهينا بسهولة من إنشاء قسم متاح ونترك بعد ذلك البرنامج (المقسّم ج) هذا شاكرين له، ونذهب إلى أيقونة التثبيت على القرص الصلب الموجودة على سطح المكتب.



سنمضي خطوات التثبيت ونكتب البيانات المطلوبة كاسم الجهاز والبلد حتى نصل إلى النقطة الحساسة وهي التقسيم، سنختار -كما في اللقطة إلى اليسار- "استخدام المساحة المتاحة"، وهذا هو الخيار قبل الأخير في مربع الحوار الذي سيظهر عند الضغط عليه في اليسار عند السهم الصغير.
ستتركك الآن مع التثبيت والاستمتاع بلينكس دون فقد بياناتك، فلم نلمس أي قسم من أقسام القرص بسوء غير أننا خصّصنا مساحة خالية نمرح فيها، وهذا يفيد أيضاً في أي قسم من الأقسام إذا كنا نريد مساحة خالية لأي غرض كالبرمجة مثلا.

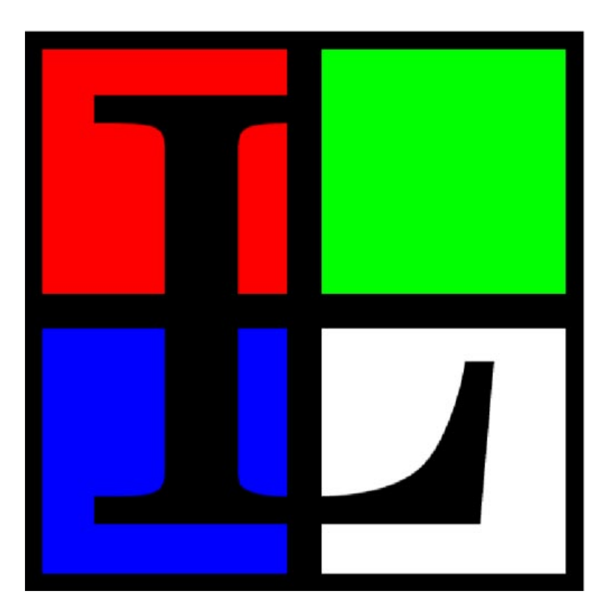


وهذا كله في تثبيت الأعجوبة. بعد التثبيت سترى محمل الإقلاع يخبرك عن أي النظامين تريد ستختار (Other) إذا كنت تريد الدخول على النظام السابق ويمكنك أن تثبت أي نظام آخر أو أي توزيعة أخرى كأوبُنتو، فلم نستخدم غير القرص الحي والبرامج الموجودة عليه، وهذا أسهل من أن تقسم كل شيء بمفردك أو ببرامج أخرى وتعيد التشغيل وخلافه. لكن إذا كنت من المحترفين يساعدك ذلك بأن تبدأ في التعديل على هذا القسم الفارغ من المساحة وتختار مساحات للذاكرة والإقلاع نفسك، وتبدأ في تنسيقهم بمفردك. ستلاحظ رسائل تأكيد عند كل تغيير افهمها ثم اضغط دون انزعاج، فأنت على الطريق السليم لأنك ببساطة في مساحة فارغة ليس عليها بيانات وهذا هو المهم عند الكثيرين. (الصورة إلى اليسار للأقسام من الداخل بجميع الأنواع).

وختاماً أرجو أن أكون قد وُفّقت في نقل المعلومات، وأشكر أسرة مجتمع لينكس وأدعو الله أن يَنفع بهذا العمل ويكون خالصاً لوجهه الكريم، والسلام عليكم ورحمة الله وبركاته.

متصفح الإنترنت الرائع : Links

إعداد : علي الشمري



أود التطرق اليوم إلى متصفح يعرفه الجميع وهو links، والذي يعمل من خلال الطرفية Terminal ولا يدعم الصور كما يعتقد الأغلبية.
لكن ما لا يعرفه الكثيرون هو أنه يوجد متصفح links ولكن يدعم الصور. من بعض مميزات هذا المتصفح :

- التشغيل بنمطين: نمط يدعم الصور ونمط لا يدعمها
- البرنامج مجاني
- البرنامج يخضع لرخصة GPL
- تستطيع تشغيله بالطرفية مع دعم الفأرة
- قوائم للتحكم بالمتصفح سواءً تم تشغيله بنمط يدعم الصور أو لا
- يدعم HTML 4.0 بدون CSS
- يدعم HTML 1.1
- يدعم الجداول والإطارات، سواءً في النمط الداعم للصور أو لا
- يدعم الصور GIF, JPEG, PNG, XBM, TIFF إذا تم تشغيله بنمط دعم الصور
- يدعم المفضلات Bookmarks
- يدعم الاتصالات Keepalive
- يقوم بعملية إعادة الاتصال في حالة انقطع الاتصال TCP

وغيرها الكثير.

لتركيب البرنامج فإنك ستحتاج إلى المكتبات التالية:

المكاتب الأساسية:

١.libpng
٢.IJG libjpeg
٣.TIFF Library
٤.SVGAlib

المكاتب الاختيارية:

١.إذا أردت دعم SSL؛ عليك إضافة مكتبة OpenSSL
٢.إذا أردت دعم المواقع المضغوطة بواسطة gzipped؛ عليك إضافة المكتبة zlib
٣.إذا أردت دعم المواقع المضغوطة بواسطة bzipped؛ عليك إضافة المكتبة libbz2

لتركيب البرنامج قم بتحميل البرنامج من الرابط:

http://links.twibright.com/download/links-2.2.tar.gz

أو

http://links.twibright.com/download/links-2.2.tar.bz2

قم بفك الضغط ودخول مجلد البرنامج:

```
$ tar xzvf links-2.2.tar.gz
```

أو

```
$ tar xjvf links-2.2.tar.bz2
$ cd links-2.2/
```

بعد ذلك، إذا كنت تريد تركيب البرنامج بدعم للصور نفذ الأمر:

```
./configure --enable-graphics --with-x
```

وإذا أردت معرفة الخيارات الأخرى:

```
./configure --help
```

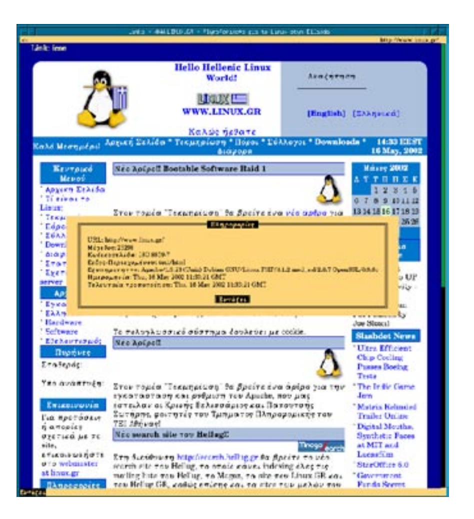
بعد أن انتهت عملية التشكيل Configuration، نفذ الأمر التالي:

```
$ make
```

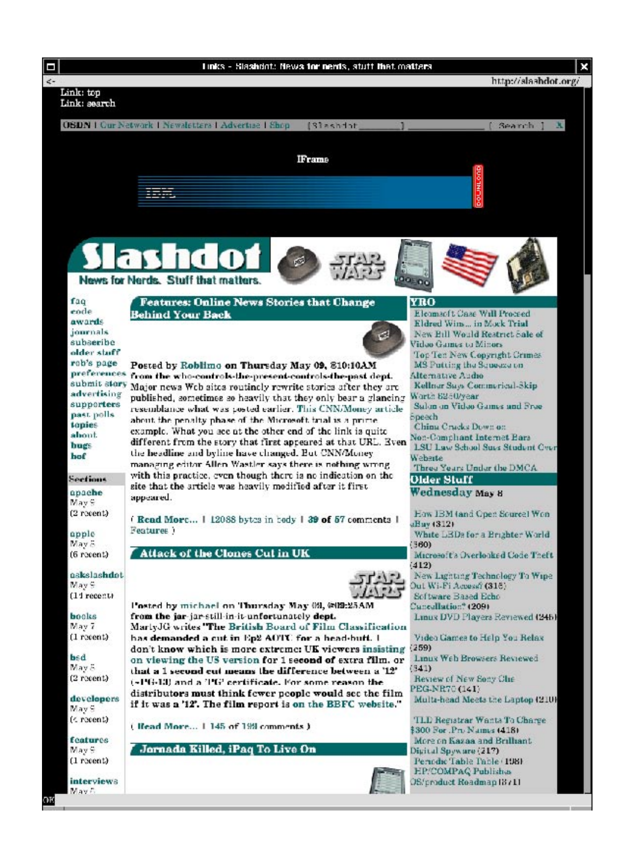
وبعدها بحساب المستخدم الجذر root أو sudo نفذ:

```
$ make install
```

فيما يلي بعض الصور للبرنامج:







الموقع الرسمي:
http://links.twibright.com

جنو/لينُكس عالم الحرية .. جنو/لينُكس عالم الطبيعة!

إعداد: حسام الدين قربوج



عصر جديد من الوعي البيئي يظهر في أيامنا هذه؛ فبعد الحديث عن ظاهرة الاحتباس الحراري وأزمة الطاقة، نواجه هذه الأيام أزمة اقتصادية عالمية ترمي بظلالها على جميع مجالات الحياة و تدعونا إلى إعادة مراجعة منظوماتنا الاستهلاكية على مستوى الأفراد والجماعات.

كيف يمكننا التصدي لهذه القضايا الخطيرة: التلوث، أزمة الطاقة، وأزمة المال؟

إضافة إلى السيارات التي تعمل بالإيثانول والتوربينات الهوائية، العديد من رجال تقنية المعلومات Information Technology وخاصة من مجتمع جنو/لينُكس والبرمجيات الحرة أبدوا استعدادهم لدعم أي فكرة أو برامج تكون أيكولوجية، أو بالأحرى بيئية، وهذه مبادرة عادية لأشخاص اختاروا الحرية من قبل؛ فمثلما آمنوا بحق الجميع في المعرفة و التقنية، ها هم اليوم يشاركون الصوت الذي يدعو للمحافظة على كوكبنا الأرض بابتكارهم لبرامج و أنظمة تشغيل مقتصدة للطاقة.

سنوضح في هذا المقال كيف بإمكان المستخدم العادي تعديل نظام تشغيله جنو/لينُكس ليقتصد في استهلاك الطاقة الكهربائية، ونشرح تقنية المحاكاة Virtualization وأهميتها في هذا المجال.
إذا كنت من محبي جنو/لينُكس ومحبي الطبيعة ندعوك لقراءة هذا المقال واكتشاف مزايا هذا النظام العجيب.

أبدأ بكلمة لشركة Canonical الداعم الرسمي لتوزيعة أُبنتو Ubuntu و التي تقول: "إن برمجة نظام أُبنتو قائمة على مجموعة من الوحدات التي تتواصل فيما بينها؛ والتي تستطيع التحكم بالذاكرة والمعالج حسب ما تقتضيه الحاجة"؛ أي على عكس نظام التشغيل Windows Vista الذي يعمل بطريقة متجانسة ويقوم بتحميل كود غير مفيد مما يزيد من استهلاك الطاقة ومساحة التخزين.

أضف إلى ذلك أن نظام التشغيل جنو/لينُكس وأغلب برمجياته مُبرمجة بلغتي سي وسي++ وبالتالي تستهلك مساحة أقل من الذاكرة عن أخرى مُبرمجة بلغات كـ Net. أو جافا.
هذان الميزتان الأساسيتان في نظام التشغيل جنو/لينُكس شجعتا مطوري البرامج على ابتكار مشاريع صديقة للبيئة ودعمها من شركات عملاقة على غرار شركة IBM في مشروع Big Green Linux و شركة Intel في مشروع Lesswatts.org.

هل تعلم أنه بإمكانك الاقتصاد في الطاقة الكهربائية التي يستهلكها حاسوبك حتى بدون أي تحديث للبرمجيات؟!
هذه بعض النصائح العملية اقترحها أفراد من مجتمع جنو/لينُكس بالتعاون مع مهندسين من شركة إنتل Intel.

على مستوى الواجهة Ethernet:

يعمل مراقب الشبكات المحلية Ethernet على نقل الإشارات في قطع طويلة من الكابل وبسرعة كبيرة. يستهلك PHY عدة Watts فقط للقيام بهذه المهمة.

Wake on LAN:

معظم أجهزة التحكم في الشبكات المحلية Ethernet لها ميزة تسمى Wake on LAN تسمح لمراقب الشبكات بإرسال حزمة سحرية قادرة على تشغيل الحاسوب عن بعد.



WOL ميزة جيدة إذا كنت تتحكم في أجهزتك عن بعد. مع ذلك فإن WOL تحتفظ ببطاقة الشبكة نشطة حتى إذا كان الحاسوب مغلقا.
الآثار الجانبية:
بعض الآثار الجانبية الناجمة عن ديمومة عمل ميزة WOL:
إذا كنت تمتلك بطاقة شبكة فى حالة عدم استعمال فإن WOL يحافظ على نشاط البطاقة بصفة معتدلة طوال الوقت. يفعل ذلك لتغطية الحالة التي تغلق فيها الحاسوب وتتركه متصلا بكابل الشبكة.
إن ظاهرة استخدام بطاقتي شبكة أو أكثر على خادم واحد كثيرة الانتشار هذه الأيام مما يجعل سيناريو وجود بطاقة ليست في حال استخدام محتملا وليس نظريا.

إيقاف ميزة WOL:
في بعض الأحيان، يحتوي الـBIOS على أوامر تُخوّل لك تعطيل أو تشغيل ميزة WOL، لكن يمكن التحكم في ميزة WOL في نظام التشغيل جنو/لينُكس عن طريق برنامج ethtool.

لتعرف هل ميزة WOL نشطة في الواجهة eth0 قم بكتابة الأمر التالي:

```
ethtool eth0
```

ستحصل على نتيجة تشبه التالية:

```
# ethtool eth0
Settings for eth0:
        Supported ports: [ TP ]
        Supported link modes:   10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Supports auto-negotiation: Yes
        Advertised link modes:  10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
        Advertised auto-negotiation: Yes
        Speed: 1000Mb/s
        Duplex: Full
        Port: Twisted Pair
        PHYAD: 0
        Transceiver: internal
        Auto-negotiation: on
        Supports Wake-on: umbg
        Wake-on: g
        Current message level: 0x00000007 (7)
        Link detected: yes
```

هذا الأمر يظهر لنا العديد من إعدادات الواجهة eth0، ومنها المتعلق بميزة WOL. في هذا المثال: العداد wake-on يحتوي على الرمز g وهذا يعني أن الواجهة مُعدّة لاستقبال الحزمة السحرية.
أما إذا كان يحتوي على d فهذا يعني أن ميزة WOL ليست نشطة على مستوى هذه الواجهة.

لتعطيل ميزة WOL في الواجهة eth0 اكتب الأمر التالي:

```
ethtool -s eth0 wol d
```

إذا كنت لا تستعمل حاسوبك إلا للإبحار على الإنترنت؛ فأنت لست بحاجة إلى واجهة سرعتها تقاس بالجيجا بايت، إلا أن أغلب حواسيبنا اليوم تدعم هذه السرعة الفائقة؛ مما يزيد من استهلاك الطاقة.

Ethtool يساعدك على التحكم في سرعة الواجهة وبالتالي كمية الطاقة المستهلكة؛ فالطاقة المطلوبة لنقل إشارة على مسافة معينة ترتفع مع ارتفاع سعة الشبكة:

الطاقة التي تستعمل محول شبكة في ربط بسرعة جيجا بايت أكبر بكثير (2 Watts أو أكثر) من الطاقة الكهربائية التي تستخدم في ربط بسرعة ١٠٠ ميجا بايت.
لهذا إذا لم تكن بحاجة إلى استعمال الواجهة بسرعة الجيجا بايت؛ يمكنك تعديلها لتصبح ١٠٠ ميجابايت عن طريق تنفيذ الأمر:

```
ethtool -s eth0 autoneg off speed 100
```

للعودة إلى سرعة ١ جيجا بايت؛ اكتب الأمر التالي :

```
ethtool -s eth0 autoneg on speed 1000
```

على مستوى واجهة الشبكة اللاسلكية Wi

تستهلك الشبكة اللاسلكية الطاقة عند الإرسال والاستقبال على حد سواء. الاستعمال النموذجي لهذه الشبكة عن طريق حاسوبك المحمول يوفر لك بعض الطاقة. سنعرض لكم بعض الحيل التي تساعدك على تخفيض استهلاكك للطاقة عند استعمالك للشبكة اللاسلكية.

نمط حفظ الطاقة:

لقد تم وضع بروتوكول استطلاع حفظ الطاقة PS-Poll للمساعدة على تقليص كمية الوقت التي يحتاج فيها الراديو اللاسلكي للطاقة.
أضف إلى ذلك فإن هذا هذا البروتوكول يخول لواجهة الشبكة اللاسلكية أن تخبر نقطة التحكم بمتى ستكون في حالة استخدام منخفض للطاقة.

في هذه الحالة تقوم نقطة التحكم بإمساك الحزم المرسلة إليها. بالطبع كلما زاد الوقت الذي تكون فيه الواجهة اللاسلكية في حالة سُبات كلما زاد اقتصادنا للطاقة.
سائق الجهاز يتحكم في مقدار الوقت المقضي قبل إعادة التشغيل الكامل للواجهة اللاسلكية واستقبال الحزم المعلقة من قبل نقطة التحكم.

بعض النقاط السلبية لهذه التقنية:

ارتفاع زمن الوصول: هذا العامل يجب أن يبقى منخفضا إذا كنت تستعمل الصوت أو تشاهد التلفاز عبر الإنترنت. يُنصح إذا بعدم تشغيل بروتوكول PS-Poll في هذه الحالة.

نشير أيضا إلى أنه هناك بعض نقاط التحكم اللاسلكية التي لا تدعم تقنية PS-Poll.
طريقة تشغيل بروتوكول PS-Poll تختلف حسب نوع الواجهة اللاسلكية.
لتشغيل نمط حفظ الطاقة اللاسلكي على واجهة تستعمل السائق ipw٢١٠٠ أو ipw٢٢٠٠؛ يمكن استعمال الأمر التالي:

```
iwpriv eth1 set_power 5
```

eth1 هو اسم الواجهة. أحيانا يمكن أن يكون eth0 أو wlan0 أو....
رقم ٥ هو الدرجة التي سيتم بها الاقتصاد في الطاقة:

١	أصغر رقم ممكن. أقل درجة لحفظ الطاقة
٥	أكبر رقم
٦	لعدم تشغيل خاصية حفظ الطاقة

على مستوى العرض و الرسوميات

لا شك أن شاشات الكريستال السائل LCD هي من أكثر المستهلكين للطاقة على حاسوبك المحمول. بالتخفيف من الكثافة الخلفية للشاشة تستطيع الحفاظ على كمية هامة من الطاقة (حوالي 5 Watts).

الحد من سطوع الضوء الخلفي:

للتحكم في سطوع الضوء الخلفي لشاشتك بنسبة ٥٠٪ يمكن استعمال برنامج xblacklight كالتالي:

```
xbacklight -set 50
```

العديد من توزيعات جنو/لينُكس تحتوي على تطبيقات يمكن أن تحل محل برنامج xblacklight.

حافظات الشاشة:

بعض حافظات الشاشة المتحركة جميلة جدا، لكن من منظور توفير الطاقة استخدام مثل هذه الحافظات ليست فكرة جيدة على الإطلاق.
أولا، حافظة الشاشة تنفق وقتا مهما من وقت المعالج المركزي (في حالة حافظات للشاشة ثلاثية الأبعاد يتم الاستعانة بمعالج البطاقة الرسومية GPU)، وتستهلك أيضا الطاقة (الأجزاء المتحركة توقظ المعالج المركزي كل الوقت للقيام بهذا العمل الثقيل).
بمثل هذه الحافظات للشاشة المتحركة؛ يمكن لحاسوبك أن يستهلك الطاقة أكثر حتى من وضع الاستخدام العادي.
التصرف الأكثر ملائمة لتوفير الطاقة هو أن توقف عمل الشاشة تماما. التقنية المتداولة لإيقاف الشاشة تسمى DPMS.

لتشغيلDPMS اكتب الأمر التالي:

```
xset +dpms
```

لإيقاف الشاشة بعد ١٢٠ ثانية من عدم الاستعمال اكتب الأمر التالي:

```
xset dpms 0 0 120
```

لايقاف عملDPMS اكتب الأمر التالي:

```
xset -dpms
```

كيف تساهم تقنية المحاكاة Virtualization في خفض كمية انبعاث غاز ثاني أكسيد الكربون؟!



إذا أردنا أن نُعرّف تقنية المحاكاة Virtualization؛ يمكن أن نقول بأنها حشد لمجهودات عمل بعض الأجهزة على جهاز واحد؛ بحيث لا نكون في حاجة إلى الاستعانة بخادم جديد لإضافة تطبيقات ما.

إن خفض حاجتنا العملية من الأجهزة يؤدي مباشرة إلى خفض حاجتنا اللازمة لتبريدها والطاقة اللازمة لتشغيلها.

كل خادم افتراضي يوفر مايقارب ٧٠٠٠ كيلو وات من الكهرباء في السنة، أي مايعادل ٤ أطنان من غاز ثاني أكسيد الكربون CO٢ .
وفي ظل ما نعيشه اليوم من أزمة حقيقية في الطاقة؛ تعتبر تقنية المحاكاة Virtualization حلا مناسبا من وجهة نظر بيئية، وحتى اقتصادية بالنسبة لأصحاب المؤسسات.

إذا قمنا باستبدال ١٠ أجهزة حقيقية بواحد ذي قدرات عالية؛ تضمن لنا تقنية المحاكاة توفير الطاقة بنسبة ٨٠ إلى ٩٠ ٪.
مع العلم بأن نسبة الاستعمال الحقيقي لقدرات الخادم تقدر بـ ١٥٪، وأن تكلفة تبريد وتشغيل الخادم الواحد تعادل سنويا قيمة شرائه.

يجدر بنا الإشارة إلى أن تقنية المحاكاة لا تقلل من قدرات الخادم على أداء العمل المخصص له.
لعل من أهم البرامج في ميدان المحاكاة برنامج Virtual Box والذي يستحق مقالا خاصا لشرحه.

الخاتمة

باستخدامنا لهذه التقنيات البسيطة نساهم في توفير استهلاك الطاقة الكهربائية بصفة مهمة وبذلك تقليص انبعاث الغازات الضارة بالبيئة.

المراجع:
www.lesswatts.org
http://www.linuxjournal.com



مراقبة ما يحدث على جهاز الحاسوب الخاص بك أثناء غيابك

إعداد : روضة الصوابني



ملحوظة هامة:
إن كاتب الموضوع ومجتمع لينوكس العربي لا يتحملان أية مسؤولية نتيجة أي استخدام غير قانوني لمحتوى هذا المقال؛ فقد تمت كتابته لأهداف تعليمية فقط.

إذا كنت تريد العمل على نظام التشغيل لينُكس، وتريد معرفة ما يحدث على جهاز الحاسوب الخاص بك حينما تكون بعيدًا عنه؛ سنقوم الآن بإعداد برنامج بسيط يقوم بالتقاط صور لسطح مكتبك كل فاصل زمني، وإرسالها إلى بريدك الإلكتروني.

هذه الطريقة ليست المُثلى ولا الوحيدة، لكن تبقى طريقة بسيطة ومفيدة حسب الاستعمال الشخصي، ولكل اختياره الخاص.

تثبيت البرنامج

أولا، يجب عليك تثبيت كل من: postfix - mutt - scrot

```
sudo apt-get install postfix mutt scrot
```

:scrot
اختصار ل SCReen shOT، وهو برنامج بسيط لالتقاط صور للشاشة باستعمال سطر الأوامر.

:Mutt
هو زبون Client بريد إلكتروني على نمط نصي Text Mode.

Postfix:
هو خادم Server بريد إلكتروني.

ضبط Postfix

بعد الانتهاء من تثبيت Postfix؛ يجب ضبط هذا الأخير حتى يتم ربطه بشبكة الإنترنت.
هذا الضبط ضروري حتى نتمكن لاحقًا من إرسال بريد إلكتروني عبر الإنترنت.

لضبط Postfix؛ سنقوم بالتالي:

١.تحديد عنوان الخادم الذي سنستعمله كمنقال للبريد (١) Mail Relay
سنقوم بالتعديل على الملف

/etc/postfix/main.cf

وإضافة أو تعديل التالي:

relayhost = [smtp.fai.fr]

smtp.fai.fr هو عنوان خادم البريد الخاص بمزود خدمة الإنترنت لديك. على سبيل المثال: smtp.planet.tn

relayhost = [smtp.planet.tn]

٢.تحديث عنوان المرسل
يجب الآن ضبط postfix لتحديث عنوان المرسل ليأخذ بعين الاعتبار عنوان البريد الإلكتروني الخاص بك وليس العنوان الذي لديك على الجهاز.
بخلاف ذلك فإن خادم البريد الخاص بك (بالنسبة لنا smtp.planet.tn) سيصله طلب تتابع من أحد المستخدمين على شاكلة login.localhost.localdomain وهو العنوان الموجود على حاسوبك.

سيتم تجاهل هذا الطلب في حالة ما لم تكن قد سجلت اسم نطاقك Domain وذلك حتى يتفادى مزود خدمة الإنترنت أن يكون نقطة تتابع بالنسبة لمواقع ال Spam أو الفيروسات.

لتحديث عنوان المرسل قم بتحرير الملف التالي:

```
gedit /etc/postfix/canonical
```

ثم نعدل:

```
yourlogin1  yourmail1@domain.com
yourlogin2  yourmail2@domain.com
```

بالنسبة لنا ستكون:

```
root raoudha@yahoo.com
raoudha raoudoutchy@gmail.com
```

ثم نعدل الملف

/etc/postfix/main.cf

كالآتي:

```
sender_canonical_maps = hash:/etc/postfix/canonical
```

هذا السطر سيشير ل postfix للأخذ بعين الاعتبار إعادة كتابة العناوين.

إثر تعديل الملف

/etc/postfix/canonical

قم بتنفيذ الأمر:

```
sudo postmap /etc/postfix/canonical
```

هذا الأمر سيمكننا من إحداث أو إعادة صياغة جدول العناوين الخاص بـ postfix

ثم نفذ الأمر:

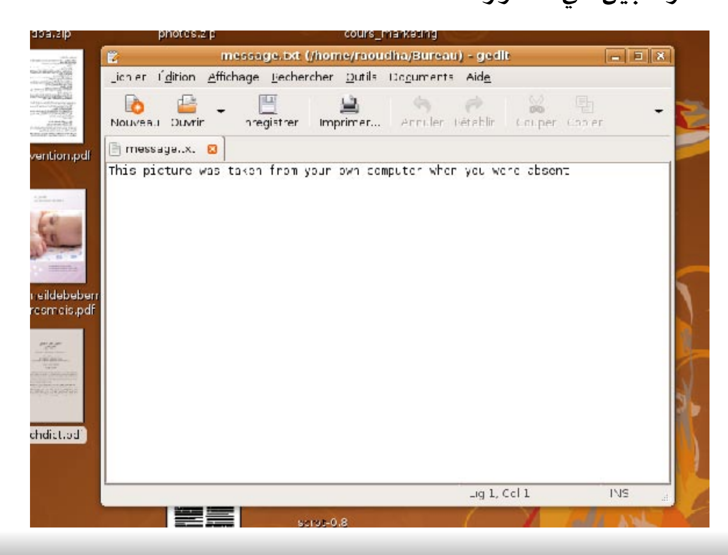
```
sudo postfix reload
```

إعداد برنامج لإرسال البريد الإلكتروني تلقائيًا

بعد ضبط postfix ، سنقوم بإعداد برنامج لإرسال البريد بصفة تلقائية على فترات منتظمة.
بدايةً، سنقوم بكتابة رسالة في ملف نصي. اكتب ما تريد فهي مجرد مضمون الرسالة التي ستصلك لاحقًا على بريدك الإلكتروني. يجب إضافة هذه الرسالة حتى لا يصلك البريد على شكل Spam.
عند تنفيذ الأمر:

```
nano /path_to/message.txt
```

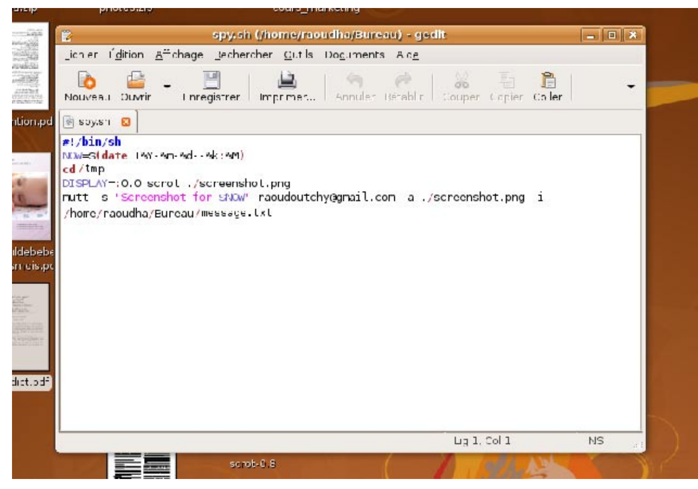
يمكنك إضافة مضمون الرسالة كما هو مبين في الصورة



أضف الملف "spy.sh" ثم احفظه في مكان لا يعرفه غيرك.
الآن أضف الأسطر التالية لهذا الملف، وقم بحفظ التغييرات:

```
#!/bin/sh
NOW=$(date +%Y-%m-%d--%k:%M)
cd /tmp
DISPLAY=:0.0 scrot ./screenshot.png
mutt -s "Screenshot for $NOW" yourmail@domain.com -a ./screenshot.png -i /
path_to/message.txt
```

استبدل youremail@domain.com بعنوان البريد الإلكتروني الخاص بك، والمسار:
/path_to/message.txt
بمسار الملف الذي يحتوي على رسالة البريد.



الآن، سنجعل الملف "spy.sh" ملفًا تنفيذيًا Executable

```
chmod u+x /path_to/spy.sh
```

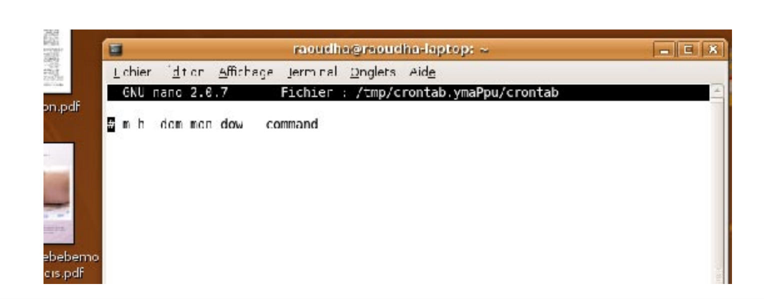
ثم نقوم ببرمجة التنفيذ عن طريق corn.
Corn عبارة عن نظام يسمح لمستخدم نظام التشغيل لينُكس بتنفيذ الأوامر على فترات زمنية محددة.
يجب الانتباه إلى ضرورة وجود الملف
/etc/cron.deny
بالنسبة لبعض التشكيلات Configurations.
لذلك سنقوم بتنفيذ الأمر التالي:

```
sudo touch /etc/cron.deny
```

إذا أردنا حجب أحد المستخدمين عن استعمال Corn؛ يمكننا إضافة اسم المستخدم إلى الملف
etc/cron.deny/
ثم، لبرمجة التقاط صورة الشاشة كل خمس ثوان مع إرسال الصورة عن طريق البريد الإلكتروني؛ نقوم بتعديل Corn كالتالي:

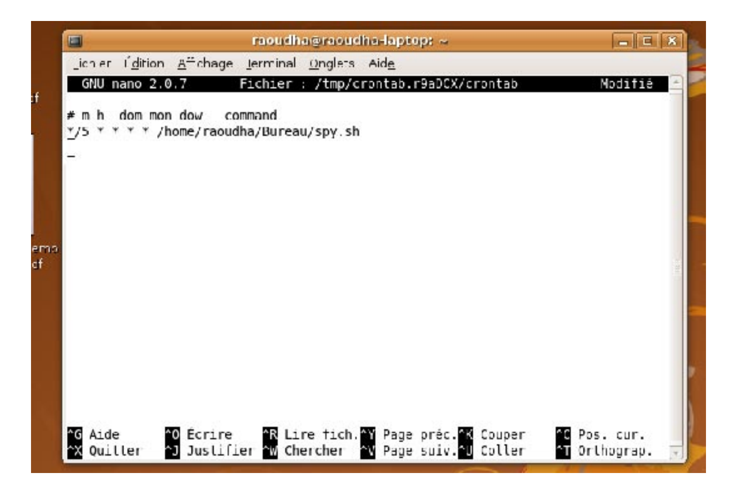
```
crontab -e
```

ستظهر لك النافذة التالية :



قم بإضافة السطر التالي:

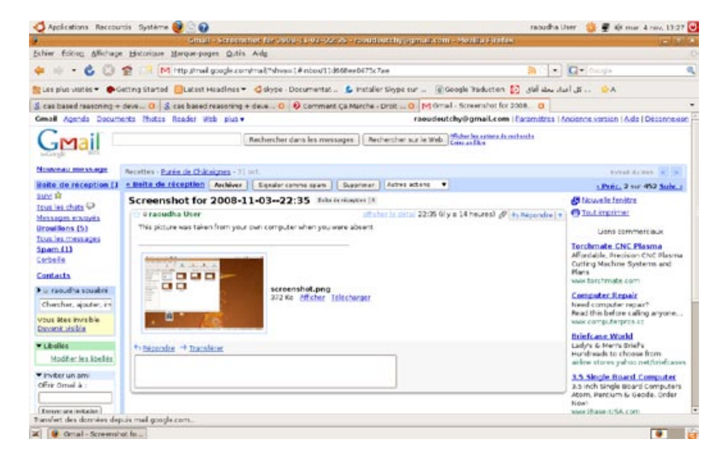
```
*/5 * * * * /parth_to/spy.sh
```



يمكنك تغيير الفترات الزمنية بين إلتقاط كل صورة بتغيير الرقم ٥ إلى عدد الثواني الذي تريده.

استقبال الرسائل

لم يبق سوى أن تراجع بريدك الإلكتروني، وتتأكد من وصول الرسائل:



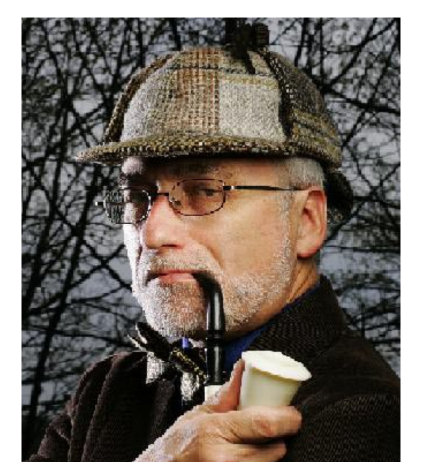
ختامًا، يمكن تطوير هذا البرنامج البسيط بحيث يقوم بإرسال مقاطع فيديو بدلا من الصور لسطح المكتب وذلك باستخدام تطبيق byzanz.

يهدف هذا المقال إلى تنمية الخبرة والتدابير الوقائية لدى القارئ، ونحن ندعو لحسن استخدام ما ورد به.

هامش

(١)منقال البريد Mail Relay:
عبارة عن خادم، غالبًا ما يكون على شبكة الإنترنت. يمكن لهذا الخادم نقل البريد من مُرسل البريد إلى الوجهة الصحيحة المرسل إليها. يقوم منقال البريد خلال هذه العملية باستخدام بروتوكول نقل البريد الإلكتروني SMTP.

من مغامرات المحقق وميرت فونلي:
اللغز الغامض للدودة الحمراء!



تأليف: بن أوكوبنيك
ترجمة وإعداد: مؤيد السعدي

"شارفنا على الوصول يا فرنك"
وميرت وفرنك كانا قد سارا على طول نفق VPN tunnel يُسمع فيه تردد قرع نعالهم راجعًا من على جدران التيتانيوم؛ وعندما وصلا إلى سعة البيئة المريحة للنظام الهدف، كان فرنك يرغب بسحب متغير مريح ويريح قدماه، لكن وميرت أصر على المتابعة. استدار وميرت ودخل الغرفة التي تحمل العنوان /var/log/apache/

"ها نحن ذا أمام /var/log/apache/access.log المسكين يصل إلى ٤٠٠ ميغابايت ويكاد يحتل كل قسم القرص مع أنه قد طوي(١) قبل أيام!"

بعد أن انزلق فرنك على الأرضية اللامعة (لأن النظام قد مُسح ب cruft) تدبر فرنك لنفسه كرسيًا دوّارًا كي يحدق متعجبًا في ملف السجل المنتفخ.
"ما الذي جرى هنا يا وميرت؟ أنا جئت لأخبرك عن التقرير في الصحيفة تلك الذي يمدحك بعد حل مشكلة قاعدة البيانات المفقودة في بنك "بج رتش" فجررتني إلى هنا قبل أن أنبس ببنت شفة، أنا لا أمانع ذلك لكن..."

ابتسم المحقق المشهور مزهوا
"أحب التركيز أثناء العمل، ألست كذلك؟! هناك ما هو أسوأ... إليك القضية: موكلنا شركة متخصصة في تصنيع مسننات اللحام لأحذية الخيل لحساب "نبكنفرنجنج" الصناعية وهم مرتابون من أشياء غريبة تحدث على موقع الويب خاصتهم، حيث تتأخر استجابة الخادم وكأنه يرسل الرد من فوق أسطح المنازل، وغالبًا ما يكون الرد برسالة الخادم مشغول، مع أنه لا توجد قفزة نوعية في أعمالهم، وحيث إن الاقتصاد اليوم لا يشجع الكماليات كالتي يبيعونها لذا..."
فرنك مقاطعًا : "لعله هجوم حجب الخدمة DoS يا وميرت."
"بالطبع". وميرت بتفكيره العميق، سحب قفازات الطباعة واقترب من الطرفية "هذه صناعة تنافسية وهذه الشركة أخذت الريادة بتلميع المنتج النهائي لكن في هكذا سوق هذه ميزة هامشية والمنافسين قد يرغبون بحجب خدمة موقع الويب لما لذلك من تضيق للهامش وقد تم تكليفنا بالبحث وكتابة تقرير عن أي شيء غريب. هذه المهمة هي مجرد جمع لبيانات إحصائية"

فلنفحص بعض الأشياء. أولا لننسخ الملف إلى حيث لا تضيق به الأشياء... ها قد وضعته في /home/woomert فنحن لا نريد خسارة أي شيء إذا دمرنا الملف بالخطأ. فلنصفر ذاك الملف ونعيد تشغيل الخادم .... أحسنت. الآن فلنعد لفحص الملف. وبما أنك تشك في هجوم حجب الخدمة ماذا تتوقع أن ترى يا فرنك؟"

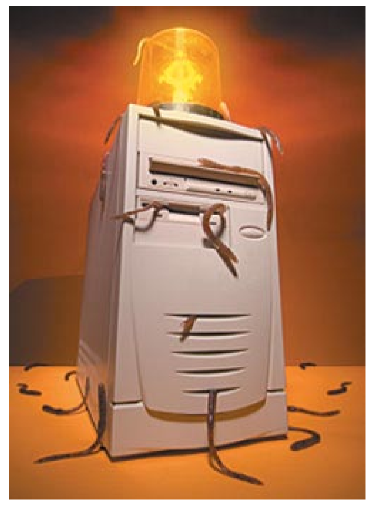
حك فرنك رأسه وعقد حاجبيه مطرقًا
"لست متأكدًا، أظن أنه علينا أن نعرف معدل ال hits لكل عنوان IP وننظر إلى القائمة مرتبة. هذا يخبرنا إن كان أحدهم يضرب الخادم ومن أين. ما رأيك ؟"

تبسم وميرت
"لماذا يا فرنك؟ إنها فكرة ممتازة... نعم فلننظر للمعدل"

```
perl -wlne'/^(\S+)/;$h{$1}++}{$a=@a=values%h;map{$b+=$_}@a;print$b/$a' access.log
12.30830039525692
```

"همممم، مثير! إذا أخذنا بالاعتبار أن الرقم سيكون كبيرًا بسبب DoS لكن هذا مجرد تخمين والرقم لا يبدو غير معقول. لعلهم يتفحصون المنتج أكثر من مرة لأنهم يشترونها مرة واحدة في العمر وهذه الشركة تقدم كفالة مدى الحياة، فلننظر إلى القائمة المرتبة"

```
perl -wlne'/^(\S+)/;$h{$1}++}{print"$h{$_}\t$_"for sort{$h{$a}<=>$h{$b}}keys%h' access.log
...
22   users.osceola.k12.fl.us
26   152.31.2.221
26   modem-140.nyc-tc01a.fcc.net
28   62.84.228.7
31   209.106.1.124
103  bdsl.66.13.44.110.gte.net
112  24-164-141-122.si.rr.com
611  nyny01hsiapat.everestbroadband.com
1085 162.66.50.6
2817 web-05.segfl.ifl.net
55055     wsip66-210-242-2.ph.ph.cox.net
71031     205.213.111.53
85120     pc-80-193-117-84-cw.blueyonder.co.uk
97000     151.138.254.21
111092    168.11.225.251
122101    syr-24-92-242-3.twcny.rr.com
155017    212.85.1.1
175990    pool-68-161-90-99.ny325.east.verizon.net
181222    1cust185.tnt15.nyc9.da.uu.net
315078    pool-141-155-115-168.ny5030.east.verizon.net
```



"حسنًا حسنًا، انظر إلى هذا! ما تقديرك يا فرنك؟"
حدق فرنك في الشاشة لوهلة ثم أومأ قائلا بكل ثقة:
"إنه هجوم حجب الخدمة. قد أمضي يومًا أو بعض يوم متصفحًا هذا الموقع لهذا أعتبر ١٠٣ و ١١٢ حالات هامشية لكن ٣١٥ ألف مرة! لعل ذلك DDoS (أي هجوم موزع تشترك فيه عدة أجهزة محاولتا إغراق شبكة أو عائل فيها) وبما أن عدد الأجهزة قليل إلا أن هذا منوط بتحقيق لاحق وربما نتصل بمزودي الخدمة ISPs لأصحاب تلك النطاقات ونحجبهم من خلال جدار النار. يا وميرت هلا رأينا على عينة من مدخلات السجل؟ لدي نظرية لتفسير ذلك لأنها إن كانت طويلة فإن ..."
نظر وميرت ثم أومأ:
"أدرك مغزاك من ذلك يا فرنك! وهي احتمالية واردة. هنا، هذا الأمر يعطيني أطول مدخلة لعنوان IP معطى:"

```
perl -lne'/^(\S+).*?"(.*?)"/
;length$h{$1}>length$2or$h{$1}=$2}{print"@a"while@a=each%h' access.log
pool-68-161-90-99.ny325.east.verizon.net GET /default.ida?XXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXu9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7
801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

نظر وميرت وفرنك إلى الشاشة ثم إلى بعضهما ثم صفقا بيمينيهما عاليًا وقد زاد عليها فرنك بأن تلوى فرقع أصابعه
"واو! لقد أحسنت بوصفها منذ البداية. ما رأيك؟"
"قد فعلتها يا فرنك، يبدو أنها نسخة معدلة من دودة مشهورة (الكود الأحمر)(٢) الجيد في الموضوع أننا لا نواجه مهاجمًا متقدمًا فمحاولة نشر الإصابة بالكود الأحمر (وهي ما وجهناه هنا) تختلف عن حجب الخدمة به الذي ما هو إلا ضرب عنوان IP محدد من خلال زحمة الشبكة، وذلك لا ينجح إلا ضد أنظمة التشغيل الأثرية وبالتأكيد لا يؤثر على نظام حديث مثل لينُكس الذي يدير هذا الموقع. فكل الضرر الذي أحدثوه هو استهلاك عرض الحزمة (عمل ازدحام) وهذا ليس سيئًا جدًا فبمجرد حجبهم من جدار النار والاتصال بمزودي الخدمة لا يبقى هناك أي موضوع نقلق عليه. وفي الحقيقة هناك الكثير من الأدوات التي تحلل وتستجيب لمثل هذه الأشياء تلقائيًا وسأنصح موكلنا بأحدها"

أطلق وميرت النتائج والتعليقات إلى موكله من خلال تمريرها في أنبوب pipe | إلى برنامج mail ثم استدار إلى فرنك وعرض عليه تناول حلويات Paglia e Fieno con Pollo e Funghi (يبدو أنها حلويات من الفطر ومعكرونة على شكل قس بزيت الزيتون) (...)
وبعد العشاء، كان فرنك يتسكع عابثًا بالكرسي الدوّار في حين كان وميررت (...)
"هذه الرفاهية!" اتكأ وميرت وقال لفرنك "هل من أسئلة أو إجابات أو تخمينات؟ ألقها علي يا صديقي."
تبسم فرنك من آخر الغرفة:
"لقد بدأت أعتاد على قراءة أسطر بيرل المنفردة لكني بحاجة لبعض المساعدة، دعني أحضر ما كتبته أنت هنا. أها، ها هو قد نسخته على جهازي الكفي"

```
perl -wlne'/^(\S+)/;$h{$1}++}{$a=@a=values%h;map{$b+=$_}@a;print$b/$a' access.log
```

- كلام:
حسنا ال wlne تفعل التحذيرات وتقرأ وتكتب كل شيء في طور السطر الذي يعري (يقص) نهاية السطر EOL قبل متن الحلقة ويضيفها بعدها و n هي الحلقة التي تدور على أسطر الملف سطرًا في كل مرة وتنفذ الكود الذي يلي e عليه. كان هذا الجزء السهل (فقد درسه perldoc perlrun مؤخرًا) الآن إلى الكود /^(\S+)/ وهو تعبير نمطي REGEX يلتقط كل ما هو غير مسافة من بداية السطر فإن كان لدينا سطر تقليدي من ملف access.log مثل:

```
127.0.0.1 - - [09/Mar/2003:22:14:46 -0500] "GET / HTTP/1.0" 200 50000 "http://localhost/" "Lynx/2.8.4rel.1 libwww-FM/2.14" webcache-01.segfl.ifl.net - - [01/Apr/2003:05:45:27 -0500] "GET / HTTP/1.0" "-" 200 5238
```

ندرك أنه يلتقط عنوان IP أو اسم العائل **hostname**. وأرى شيئًا عملناه من قبل **$h{$1}++** وهو عداد التكرار، أليس كذلك؟"
تابع فرنك بعد أن ابتسم له وميرت مُقرًا

"حسنًا. **$1** هو متغير تعمله بيرل يحمل أول مجموعة أي محتويات أول زوجين من الأقواس في نمط regex وفي حالتنا هو عنوان ال IP لذا فإنك قد زودت العنوان كمفتاح للمقطع (٣) المسمى **%h** وقمت بزيادة القيمة المقابلة لكل عنوان في كل مرة يرد فيه. ثم... امممممممم... ثم هذه إغلاق الحاصرة لوحدها... لا أفهمها ولا حتى لماذا تعمل. ألا يجب أن تكون خطأ في الصياغة؟"
تبسم وميرت:

"غالبًا الحاصرة المنفردة هي خطأ في الصياغة لكن افتح perldoc perlrun وألق نظرة على المدخلة المقابلة ل **p-**:

```
# From ``perldoc perlrun''
   while (<>) {
       ...              # your program goes here << البرنامج هنا
   } continue {
       print or die "-p destination: $!\n";
   }
```

لاحظ "البرنامج هنا" فماذا يحدث لو أغلقت الحاصرة هناك؟"
ركز فرنك في الكود ثم أضاء وجهه: "فهمت فهمت! إذا أغلقنا الحاصرة هناك فنحن ننهي عبارة طالما while الضمنية وفتح حاصرة بعدها يعمل لبنة خارج الحلقة أي أنك فعلت ذلك لوضع الكود خارج الحلقة وكأنك استعملت. **END{}** رائع يا وميرت!" (٤)

وما بقي ليس صعبًا، فلنلق نظرة: **$a=@a=values%h;** حسنًا هذه تستخرج كل القيم من المقطع والتي هي العدادات وتجعل **$a** هي عدد تلك القيم وهذا ما تحصل عليه عندما تضع مصفوفة في سياق عددي (بل هي أعقد من ذلك لكن هذا هو الجزء الذي يهمنا من الموضوع)
ثم تجمع كل تلك القيم. **map{$b+=$_}@a;** حيث الدالة map تدور على كل عنصر في **@a** وتزيد **$b** بمقدار تلك العناصر وأخيرًا وليس آخرًا **print$b/$a** تطبع النسبة بين المجاميع وعدد القيم أي نقسم عدد الوصول hit لكل عنوان IP على عدد العناوين. ما رأيك؟ كيف رأيتني؟"
وقد تلون فرنك مبتسمًا بعد تصفيق وميرت وتهليله: "شكرًا شكرًا! أظن أن قضائي للوقت أدرس تحت إشراف وميرت بدأ يثمر، شكرا يا وميرت! بقية الأسطر مشابهة نوعا ما:"

```
perl -wlne'/^(\S+)/;$h{$1}++}{print"$h{$_}\t$_"for sort{$h{$a}<=>$h{$b}}keys%h' access.log
```

الجزء الأول قد علمناه فهو يحصي التكرار لكل عنوان IP. لكن في اللبنة الأخيرة (بعد الحلقة) قمت بأمر مختلف هذه المرة وسأقرأها من اليمين لليسار كما علمني وميرت: **sort{$h{$a}<=>$h{$b}}keys%h**

حسنا في هذه المرة استخرجت المفاتيح مرتبًا إياها بحسب القيم لأن { ... }(for (values %h لا تصلح لأننا نحصل على القيمة بدلالة المفتاح ولا يمكن أن نقوم بالعكس لأن القيم قد لا تكون فريدة وقد غيرت الإجراء المتبع في الترتيب sort تمامًا كما في الشرح الموجود في مخرجات perldoc -f sort أي إنك ترتب المفاتيح بحسب القيم المقابلة لها ويكون هذا باستخدام متغيري $a و $b اللذان يمثلان عنصرين سيتم ترتيبهما. وبالمحصلة حصلنا على قائمة مرتبة حسب القيم المقابلة للمفاتيح ثم طبعت تلك القائمة مع بعض التنسيق "for print"$h{$_}\t$_ وهي حلقة for على المفاتيح التي رتبناها دون متغير فيكون المتغير التلقائي _$ هو المفتاح الحالي وطبعنا $h{$_} الذي هو ما يقابل المفتاح من قيمة ثم علامة جدولة TAB ثم المفتاح الذي هو عنوان IP أو Hostname. وهذا كله طبع قائمة بالعناوين مرتبة بعدد مرات الوصول hits.
وأخيرًا لدينا هذا:

```
perl -lne'/^(\S+).*?"(.*?)"/
;length$h{$1}>length$2or$h{$1}=$2}{print"@a"while@a=each%h' access.log
```

واو هذه صعبة! حسنًا التعبير النمطي ليس سيئًا لتلك الدرجة /"(.*?)"?*.(+S\)^/ فهو يأخذ عنوان IP كسابقه ثم أي شيء إلى أول علامة اقتباس مزدوجة " أما علامة الاستفهام التي تلي * فهي تجعل التعبير في الطور غير الجشع مما يضمن لنا تلك أول علامة اقتباس مما يجب علامة الاقتباس تأخذ نص طلب HTTP Request وهو ما نريده ثم ... أوبس وميرت! بعض المساعدة!
استخرج وميرت من جيب قميصه قلم الليزر بتثاقل وأشار:
"أظنك تقصد هذا؟ length$h{$1}>length$2or$h{$1}=$2 ما كنت أريده منه هو حفظ أطول قيمة. مما يعني أن علي مقارنة القيمة الحالية المقابلة للعنوان بالقيمة الجديدة إلا أن القيمة الأولى لا تكون معرفة مما سيعطينا خطأ إذا قارنا شيئًا مع undef هذا إلى جانب وضع @a سيتسببان بظهور تنبيهات من بيرل ولتجنب رؤيتها لم أستعمل -W يجب أن لا تفعل هذا إلا إذا كنت تدرك عواقب ما تفعل (انظر perldoc perllexwarn للمزيد) الطريقة بسيطة أقارن طول القيمة الحالية المقابلة للمفتاح فإن كانت أكبر أحللت الجديدة (وهي $2) مكانها. لاحظ أني استعملت عملية أو اللينة soft or وليس أو المنطقية || لأنها لا تعمل هنا. هلا أكملت؟" أومأ فرنك "نعم، ما يقي سهل."

print"@a"while@a=each%h

رأيتك تفعلها سابقًا. نعم إنها حلقة لكل عنصر while each تدور على كل زوجين من المفاتيح والقيم داخل المقطع وتضعهما في مصفوفة وتطبع تلك المصفوفة ولأنك وضعت علامة اقتباس مزدوجة حول المصفوفة فسيتم وضع مسافة بينهما وبكلمات أخرى فإنك تطبع المقطع دون أي ترتيب وهذا غير مهم حيث إننا نريد فقط رؤية أي منها. أصحيح ذلك؟!"
"جيد جدًا يا فرنك سأعتمد على مساندتك في المرات المقبلة فهل أنت مستعد؟"
"أتمنى ذلك" نظر فرنك بكل ثقة "أعتقد ذلك، سأقوم بأفضل ما لدي. سأتوجه إلى البيت وأتركك تمضي وقتًا ممتعًا" (...)

الهامش:
كل شيء في القصة يمكن أن يكون خيالا أو مجازًا إلا أوامر لغة بيرل فإنها تقوم فعليًا بما هو مذكور في القصة. بعد قراءتي لعدد من هذه القصص أصبحت مثل المحقق وميرت أحل أعقد المشاكل بسطر من لغة بيرل. يبدو لي أن المحقق وميرت ليس إلا شخصية المؤلف بن أوكوبنك فهما يشتركان في الصفات الجسدية والشخصية. تجد القصة الأصلية في العدد ٩٠ من مجلة Linuxgazaette :

http://linuxgazette.net/issue90/okopnik.html

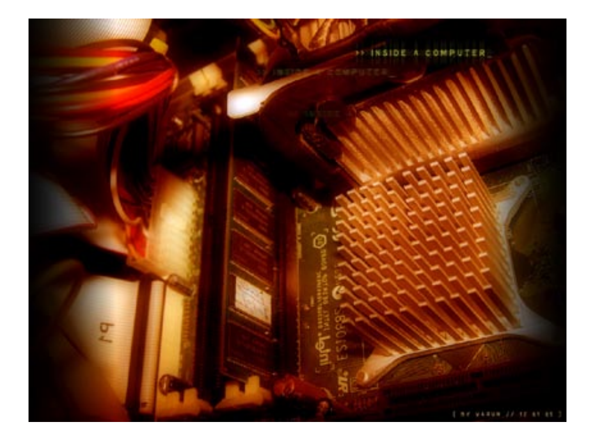
(١) طوي ملف التقرير log file rotation تعني بدء ملف جديد مع حذف أو ضغط الجزء الحالي.
(٢) الهجوم الذي استخدم في تعطيل البيت الأبيض بعبارة "اخترقه الصينيون" انظر:

http://www.ciac.org/ciac/bulletins/l-117.shtml

(٣) ويسمى أيضا قاموس نوع من البيانات يشبه المصفوفة لكنه غير مرتب ويتم الوصول للقيم من خلال مفتاح فريد.
(٤) لا وميرت و لا مراسلنا يدعي اكتشاف هذه الحركة بل هي ل Abigail في comp.lang.perl.misc وحقيقة فإن وميرت قد تأثر كثيرا بما كان ينشره Abigail.

خدمات النظام: نظرة عن قرب

إعداد : محمد الخياري



السلام عليكم ورحمة الله قراء مجلة مجتمع لينكس العربي، سأحاول في هذا الموضوع التقرب أكثر من خدمات النظام وكيفية التعامل معها بالنسبة للمبتدئين في نظام لينكس.

عند أول اتصال مع الخدمات على توزيعة ماندريفا يمكننا إلقاء نظرة على الواجهة الرسومية الواضحة والسهل استخدامها لإعداد الخدمات، ونستطيع الوصول إلى الركن المخصص للخدمات في مركز تحكم ماندريفا (MCC) بالتوجه إلى:
Menu > Outils > Outils système > Configurer votre ordinateur > Système > Gérer les services système

أو بطريقة سهلة، من خلال سطر الأوامر نكتب -بصلاحيات الجذر طبعًا-:

```
[root@mohamed]# drakxservices
```

سنلاحظ ظهور الواجهة الرسومية لإعداد الخدمات، والتي تضم معلومات عن خدمات النظام مقسمة إلى أعمدة لتسهيل الاستخدام.

العمود الأول؛ يضم اسم الخدمة.
العمود الثاني؛ يضم المؤشر actif (مُفعّل)، أو arrêté (مُتوقف).
العمود الثالث؛ عبارة عن أزرار يمكن بالضغط عليها إلقاء نظرة بسيطة على بعض المعلومات التي تخص الخدمة.
وبعد العمود السابق؛ تأتي خانات يمكن تفعيلها أو إلغاء تفعيلها، تُسمى au demmarage (عند بدء التشغيل) متبوعة بزرّين demarrer (تشغيل) و arrêter (إيقاف)، يوضحان ما يمكن للخدمة القيام به: يمكن تشغيلها وإيقافها، ويمكن أيضًا اختيار تفعيل التشغيل التلقائي للخدمة عند تشغيل الجهاز أو إلغائه.

لكن، ماذا تعني الخدمة؟
الخدمة لا تحتاج لمعلومات آتية من المستخدم (تعمل في الخلفية) على خلاف ما هي عليه البرامج المعتادة، إلا في التشغيل والإيقاف، وهذا أيضًا يمكن جعله تلقائيًا.

أوامر الخدمات و chkconfig:

الأمر service يمثل سكربت شِل بسيط تحت المجلد /sbin، ويستخدم لإظهار حالة الخدمات للتمكن من تشغيلها أو إيقافها.
هذه الخدمة تستلزم اسم الخدمة (والتي هي اسم لملف موجود داخل المجلد /etc/init.d) وتستلزم أيضا ما يجب القيام به، يعني تشغيل أو إيقاف لهذه الخدمة، وهذا ما يعطينا الأوامر بالصيغة التالية:

```
[root@mohamed]# service service_name restart
[root@mohamed]# service service_name status
```

تنبيه: الأمر service ليس له تأثير دائم، وتعود التغييرات التي أجراها كما كانت بعدما نعيد تشغيل حساب المستخدم. بينما الأمر chkconfig يظهر، ويضيف، ويحذف، ويقوم بإعداد دائم وليس مؤقتًا للخدمات.

لتشغيل إحدى الخدمات تلقائيًا عند بدء تشغيل الجهاز، نستطيع استخدام الأمر التالي:

```
[root@mohamed]# chkconfig service_name on
```

ولتفادي التشغيل التلقائي لإحدى الخدمات، نطبِّق:

```
[root@mohamed]# chkconfig service_name off
```

لإظهار جميع الخدمات وإعداداتها الحالية نطبق الأمر chkconfig --list.
(Marche =يعمل ، arrêt = متوقف)

```
[root@mohamed]# chkconfig --list

acpi 0:arrêt 1:arrêt 2:marche 3:marche 4:marche 5:marche 6:arrêt
acpid 0:arrêt 1:arrêt 2:arrêt 3:marche 4:marche 5:marche 6:arrêt
alsa 0:arrêt 1:arrêt 2:marche 3:marche 4:marche 5:marche 6:arrêt
anacron 0:arrêt 1:arrêt 2:marche 3:marche 4:marche 5:marche 6:arrêt
apmd 0:arrêt 1:arrêt 2:marche 3:marche 4:marche 5:marche 6
```

لقد أعطينا جزءًا بسيطًا لأحد المخرجات الممكنة. الخَرْج يوضح تفاعل خدمات النظام في كل مستوى من مستويات الحماية بواسطة أرقام -كما هو موضح أعلاه-.
وللتأكد من حالة إحدى الخدمات على كل مستويات الحماية، نطبِّق الأمر:

```
[root@mohamed]# chkconfig --list service_name
```

مثال:

```
[root@mohamed]# chkconfig --list anacron

anacron 0:arrêt 1:arrêt 2:marche 3:marche 4:marche 5:marche 6:arrêt
```

كل ما يظهر خلال استعمال هذه الأوامر بالخيار list-- سيصبح واضحًا أكثر خلال قراءتكم للفقرات التالية. لمعلومات أكثر عن الأمر السابق يُمكن مراجعة man chkconfig .
الأوامر المستخدمة تتطلب من المستخدم أن يعمل بصلاحيات الجذر. لا أحد يجبركم على استخدامها بدل مركز التحكم أو البرامج الرسومية المخصصة لهذا الغرض، فهذه الأوامر كما هو معروف تسهِّل الوصول بسرعة إلى الهدف فقط.
مراقبة الخدمات وإعدادها لها مزايا عديدة، نذكر منها:

التقليل من استهلاك موارد النظام:

هذا ينطبق على الخدمات من نوع daemons لأنها في غالب الأوقات نائمة، لكنها تستهلك قدرًا من موارد النظام، وهنا يأتي دور الأمر service الذي نستطيع من خلاله تشغيل خدمة الطباعة مثلًا وإيقافها عندما ننتهي من طباعة ما نريد.

تحسين إقلاع النظام:

الخدمات من نوع daemons تقوم بالتنصُّت على عدد من المنافذ، يعني كلما زاد عدد الخدمات التي تقوم بالتنصت كلما زادت المنافذ المفتوحة، وبالتالي يزداد احتمال الهجمات على هذه المنافذ، وقد نجد بعض الخدمات التي تحسن من حماية النظام.

تجنب إعادة تشغيل النظام:

إذا غُيِّرت إعدادات إحدى ال daemons فإن هذا الأخير غالبًا ما يستوجب إعادة تشغيل النظام، لتُطبَّق التغييرات التي أُجريت. عند تثبيت إحدى الحزم التي تتضمن خدمة ما، لا تقلع هذه الخدمة مباشرة، لكن تعمل بعدما نعيد تشغيل النظام. هنا نستطيع استخدام الأمر service لإقلاع الخدمة دون إعادة تشغيل النظام.

التقليل من الوقت المستغرق في إقلاع النظام:

جزء مهم من الوقت المستغرق في إقلاع نظام لينكس يُستهلك من طرف عملية إقلاع الخدمات فإذا أُعِدّ النظام ليقوم بتفعيل الخدمات المهمة فقط، نستطيع بذلك التقليل من زمن الإقلاع بشكل ملحوظ.

فهم وتخصيص إقلاع الخدمات:

هذا الجزء يهم كل شخص لا يسعد فقط باستخدام الأشياء ولكن سعادته تكمن في فهم كيفية عمل هذه الأشياء وسبب كونها على هذا الشكل. طبعًا نستطيع التأقلم مع لينكس بدون التطرق إلى ما سبق ذكره، لكن -بنظري- أجد الأمر مهمًا إلى حد ما. مهم أن نأخذ فكرة عن المفاهيم التي تختبئ وراء خدمات النظام، ولم لا، قد يأتي يوم يقوم كل منا بتطوير خدمة لتسهيل عمل يقوم به.

السكريتات المتعلقة بالخدمات:

من باب الفضول بحثت في الموضوع وكيف يقوم النظام بمعرفة الخدمات المتاحة.

السكربتات المسؤولة عن إدارة الخدمات نجدها في المسار /etc/rc.d/init.d ، ولتتمكن أدوات النظام من مراقبة صحيحة للخدمات، فمن الضروري أن هذه الأخيرة تكون هي أيضًا مراقبة من طرف أحد السكربتات الموجودة داخل المسار المذكور أعلاه.

يتضمن السكربت -المسؤول عن إدارة إحدى الخدمات- أوامر الإقلاع، على الأقل لإيقاف وتشغيل الخدمة بالسؤال. نلقي نظرة هنا على نموذج القاعدة لسكربت يقوم بالعملية التي ذكرناها:

(لأني أستخدم الواجهة الفرنسية فسأشرح المصطلحات والجمل الفرنسية، لكي يتسنّى للجميع استيعاب ما نقوم به.)

```
#! /bin/sh

# chkconfig: niveaux_d_exécution numéro_du_lien_de_démarrage numéro_du_lien_d_
arrêt
# description: brève description de ce à quoi sert le service

. /etc/rc.d/init.d/functions

case "$1" in
            start)
            echo -n "Démarrage du service: "

            echo
            ;;

            stop)
            echo -n "Arrêt du service: "
            commande(s) pour arrêter le service
            echo
            ;;

            status)
            status nom_du_service
            ;;

            *)
            echo "*** Usage: nom_du_service {start|stop|status}"
            exit 1
esac

exit 0
```

(مستوى التنفيذ ورقم رابط التشغيل وأيضًا رقم رابط الإيقاف) — (وصف الخدمة)



Démarrage du service= تشغيل الخدمة
commande(s) pour démarrer le service =أمر (أوامر) تشغيل الخدمة
status nom_du_service = حالة اسم-الخدمة
Arrêt du service = إيقاف الخدمة
commande(s) pour arrêter le service= أمر (أوامر) إيقاف الخدمة
Usage = الاستخدام
nom_du_service = اسم-الخدمة

الروابط مع مستويات التنفيذ (Runlevel):
بعض الخدمات تحتاج لخدمات أخرى للعمل، مثلا خدمة httpd (خادوم وِب أباتشي) لا يعمل بشكل جيد إذا كان سكربت network غير مفعّل. كيف إذًا يحدّد ترتيب تفعيل الخدمات خلال إقلاع النظام؟

نلقي نظرة أولًا على محتوى المجلد /etc/rc.d

```
[root@mohamed]#   ls /etc/rc.d

init.d/ rc* rc0.d/ rc1.d/ rc2.d/ rc3.d/ rc4.d/ rc5.d/ rc6.d/ rc.local*
rc.sysinit*
```

نلاحظ هنا عددًا من ملفات ومسارات يبدأ اسمها بـ rc (وهي اختصار لـ"نفِّذ أمرًا" (Run Command) بالإنكليزية). أغلب هذه الملفات والمسارات يمكن الولوج إليها من خلال روابط داخل المسار /etc.
مثلًا، إذا تفحصنا أحد المسارات التي على شكل rc <number>.d سنجد عددًا من الملفات بعضها يبدأ بالحرف S والبعض الآخر بالحرف K، كلا الحرفين K وS يتبعان بعدد مكون من رقمين، Sهو اختصار لـStart (ابدأ) والحرف K اختصار لـKill (اقتل)، والعدد الذي يتبع الحرف k وS يمثل ترتيب التشغيل والإيقاف الخاص بالخدمات.هذه الملفات كلها عبارة عن روابط للسكربتات الموجودة تحت /etc/init.d .

مثال **S17alsa** هو رابط للسكربت **/etc/init.d/alsa** ويُنفّذ بعد تشغيل **S14acpid** (وهو رابط أيضًا للسكربت **/etc/init.d/acpid**) لكن قبل **S18sound**.
نلقي نظرة أخرى على الأسطر الأولى للسكربت network:

```
#! /bin/bash
#
# network       Bring up/down networking
#
# chkconfig: 2345 10 90
# description: Activates/Deactivates all network interfaces configured to \
#              start at boot time.
```

ما يهمنا هنا هو السطر **# chkconfig: 2345 10 90**
السطر يعني أن هذا السكربت سيُنفّذ على مستويات التنفيذ (runlevel) ٢،٣،٤ و٥ مع الأولوية ١٠ ويتوقف هذا السكربت في مستويات التنفيذ الأخرى (٠، ١ و٦) مع الأولوية ٩٠

من جهة أخرى -وآليًا- سنجد رابطًا تحت اسم **K90network** داخل المسارات **/etc/rc.d/rc.6** و**/etc/rc.d/rc.1** ،**/etc/rc.d/rc.0**

ما هي مستويات التنفيذ أو runlevel ؟

مستويات التنفيذ نجدها محددة داخل الملف **/etc/inittab**

```
# Default runlevel. The runlevels used by RHS are:

   # 0 - halt (Do NOT set initdefault to this)
   # 1 - Single user mode
   # 2 - Multiuser, without NFS
   # 3 - Full multiuser mode
   # 4 - unused
   # 5 - X11
   # 6 - reboot (Do NOT set initdefault to this)
```

دائمًا وفي كل لحظة نجد النظام يعمل في إحدى هذه المستويات وغالبًا في المستوى ٣ (سطر أوامر بحت) أو في المستوى ٥ (واجهة الرسومية). المستوى ١ مخصص لأعمال الصيانة.

خلال كل تغيير من مستوى لآخر يُنفّذ السكربت /etc/rc.d/rc. هذا السكربت يمرُّ على كل الروابط الموجودة داخل نفس مسار مستوى التنفيذ الذي تم التغيير إليه ليتمكن من تنفيذ (S) أو إيقاف (K) الخدمات.

هذا يفسر لماذا المسارات /etc/rc.d/rc.6 و /etc/rc.d/rc.0 تحتوي أساسًا على روابط تبدأ بالحرف Kبما أن جميع الخدمات يجب أن تتوقف في المستوى ٠ والمستوى ٦ .

هذا النظام المعقد يسمى بعملية بدء النظام V، لأنه أُدخل في النسخة ٥ لنظام يونِكس. إذًا فكل توزيعات لينكس الأم والتوزيعات المبنية عليها تستخدم هذا النظام، ما عدا توزيعة سلاكوير؛ التي تتبع نظام البدء **BSD-style** الخاص بنظام بي إس دي.

تم بحمد الله.

ملاحظة : التوزيعة المستخدمة: MANDRIVA FREE 2009.0



تشفير نظام الملفات/الملفات باستخدام TrueCrypt

إعداد: علي الشمري



بعض البيانات الموجودة على حاسوبك هي لاستعمالك الشخصي وليس للعامة الاطلاع عليها أو استعمالها.
ملفات حسابية لشركتك، الشركات التي تتعامل معها في تجارتك، ملفات للعائلة وصور لهم أو حتى أية ملفات أخرى مهمة خاصة بك ولا تخص أحدًا سواك. وقد تتعرض للكثير من المشاكل نتيجة سرقة هذه البيانات الخاصة.
حالات سرقة البيانات وطرقها كثيرة. ربما أبرزها هي عند بيعك لجهازك المحمول والذي تقوم بحذف البيانات التي عليه وتظن أن هذا كافٍ لإزالتها نهائيًا، بينما الحقيقة غير ذلك؛ فباستخدام الأدوات الصحيحة والطرق الصحيحة تستطيع استرجاع جميع البيانات التي كانت على حاسوبك حتى لو قمت بعمل تهيئة Format للبيانات. أيضًا سرقة حاسوبك المحمول أمر بسيط ويحدث كثيرًا، وبالتالي ذهبت كل البيانات التي عليه.
إذا أخذنا هذه الأمور بعين الاعتبار؛ فإنه من اللازم أن نجد طريقة لحماية بياناتنا. السؤال الذي ربما يطرح نفسه الآن هو: كيف نقوم بذلك؟!
والجواب: عن طريق تشفير البيانات.

في هذه المقالة سنلقي نظرة سريعة على برنامج يعمل على العديد من أنظمة التشغيل: Linux و OS X وحتى Windows والذي هو TrueCrypt.

نستطيع استعمال TrueCrypt لعمل نظام ملفات قابل للتشفير بشكل فوري **on-the-fly** والمحافظة عليه. معنى أن يكون التشفير بشكل فوري **on-the-fly** هو أن تحدث عمليتي التشفير وفك التشفير بشكل آلي Automatic قبل أن يتم تحميل هذه البيانات أو تخزينها وبدون تدخل من المستخدم نفسه.

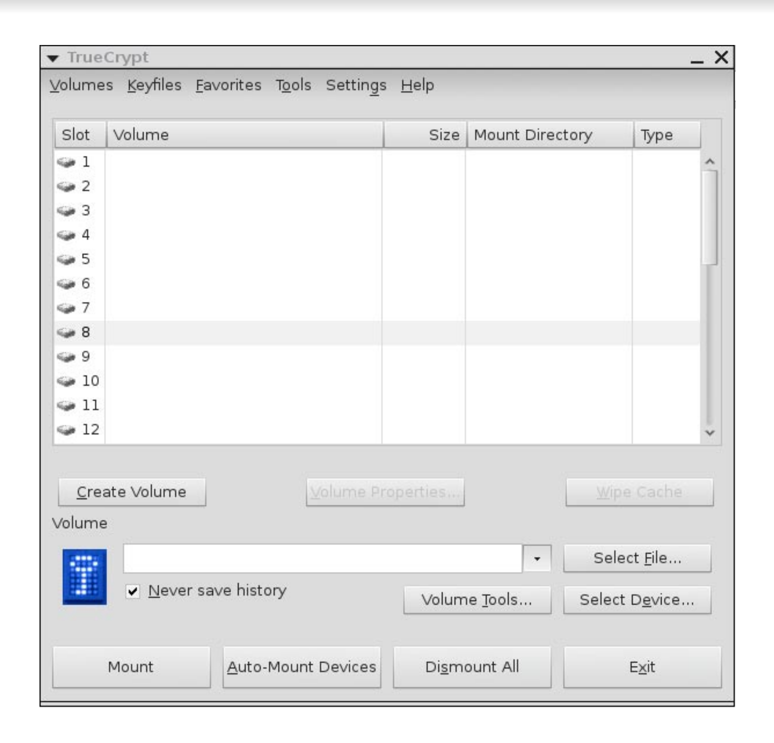
جميع البيانات التي على نظام الملفات المشفر هذا لا تستطيع قرائتها بدون استعمال كلمة السر أو المفتاح الصحيح. جميع عمليات التشفير هي تلقائية وتحدث بشكل فوري وبشفافية؛ أي بدون معرفة المستخدم حول حدوث ذلك.
TrueCrypt قادر على استعمال خوارزميات التشفير: AES و Serpent و **Twofish**. كما يدعم Hashing أي الثرم: **RIPEMD-160** و **SHA-512** و Whirlpool.

تستطيع تشغيله في نمط Traveler؛ وذلك لكي لا تكون بحاجة إلى تركيب TrueCrypt على الجهاز الذي ستقوم بتشغيله منه، وهذه تفيدنا في عملية تشفير وسائط التخزين التي تعمل عن طريق الـ USB، فتستطيع تشفير بياناتك التي عليها واستعمالها على مختلف الأجهزة بدون الحاجة إلى تنصيب TrueCrypt على جهاز الحاسوب.

يمكنك تحميل TrueCrypt عن طريق الرابط التالي:
http://www.truecrypt.org/downloads.php

اختر الحزمة التي تناسب توزيعتك. إن لم تجد الحزمة المناسبة عليك أن تقوم بتركيب البرنامج من المصدر (راجع ملف "Read Me" لمعرفة كيفية عمل ذلك).

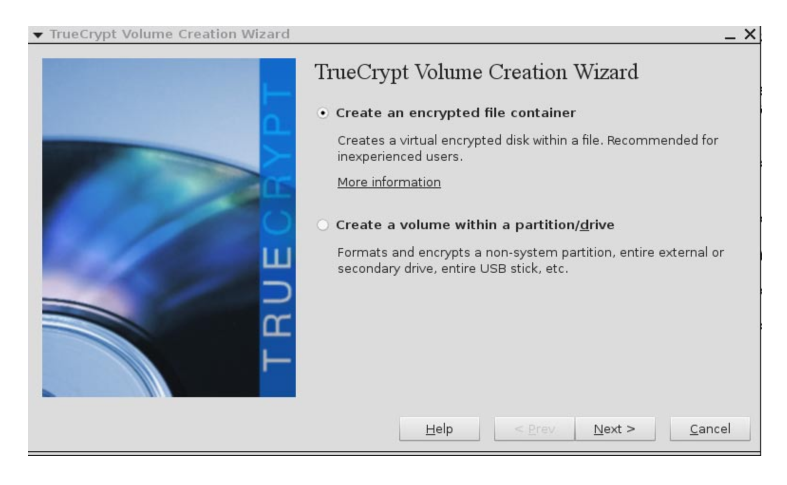
ملاحظة مهمة: مكتبات FUSE أساسية لتنصيب برنامج TrueCrypt.



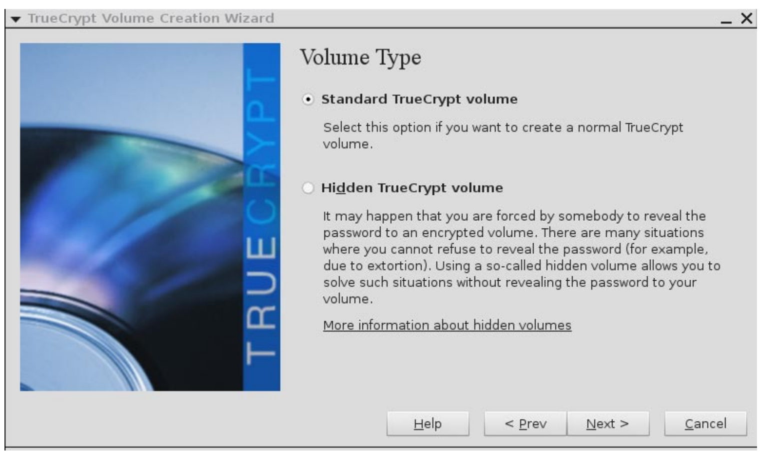
يعمل البرنامج من خلال الطرفية Terminal والواجهة الرسومية.
بشكل أساسي يعمل من خلال الواجهة الرسومية ويعود إلى الطرفية في الحالة استوجب الأمر ذلك، أو استعمل الأمر t- لإجباره على العمل من خلال الطرفية Terminal.
يستطيع TrueCrypt القيام بتشفير أجهزة التخزين/الأجزاء Partitions بكاملها أو عمل ملف تخيلي مشفر عليها.

ملاحظة:
يجب أن تعلم أن عند عملك جزء Partition بواسطة TrueCrypt فإن جميع البيانات التي عليه تُحذف. عليك أولا إنشاء الجزء ثم إضافة البيانات إليه.

عند تشغيل البرنامج ستظهر لك الواجهة الموضحة إلى اليسار.



لعمل جزء Partition جديد مشفر من خلال الواجهة الرسومية.
انقر على Toold ومن ثم Volume Creation Wizard.
ستظهر لك الشاشة التالية:

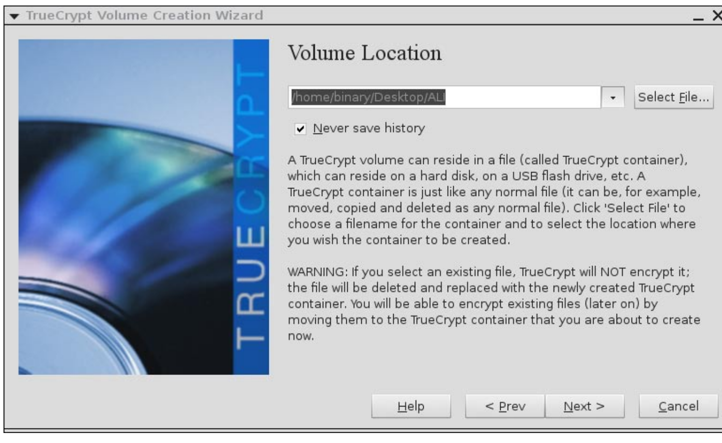


Create an encrypted file container
لعمل جزء تخيلي مشفر بداخل ملف، وهو الذي يُنصح به لمن لا خبرة له.

Create s volume within a partition/drive
لعمل تهيئة Format لجزء غير تابع للنظام (ليس عليه مجلد من المجلدات الأساسية للنظام مثل var أو / أو home)، أو لقرص صلب خارجي أو USB وغيرهم.

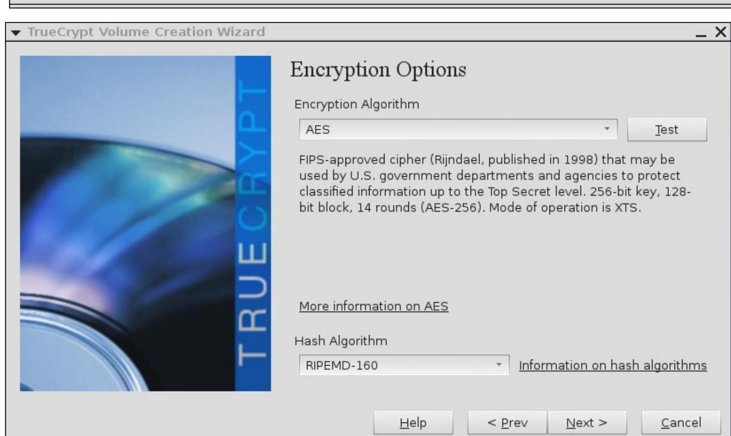
قم باختيار الخيار الأول، ثم اختر Standard TrueCrypt Volume (كما توضح الصورة إلى اليسار)

الآن قم بتحديد المكان الذي تريد تخزين الملف فيه (الصورة إلى اليمين) :

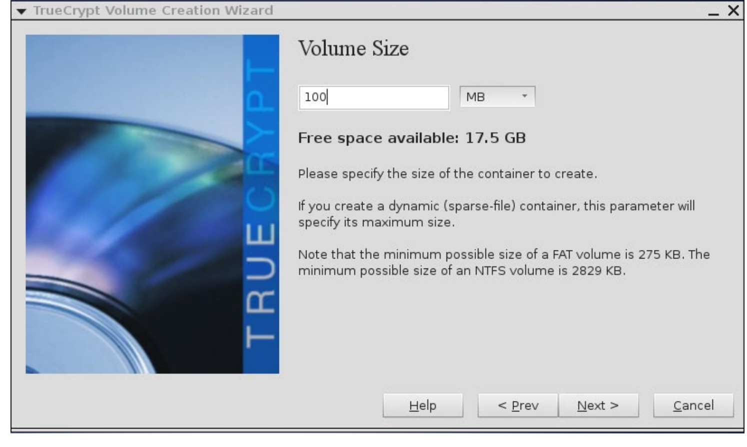


ملاحظة مهمة:
في حالة اختيارك لملف موجود أصلا فإنه لن يتم تشفيره بل سيحذف ويُستبدل بآخر. اقرأ التعليمات الموضحة جيدًا.

الآن قم بتحديد خوارزمية التشفير التي تود استعمالها وخوارزمية ال Hash أيضًا. الخيارات الافتراضية جيدة في كثير من الأحيان.

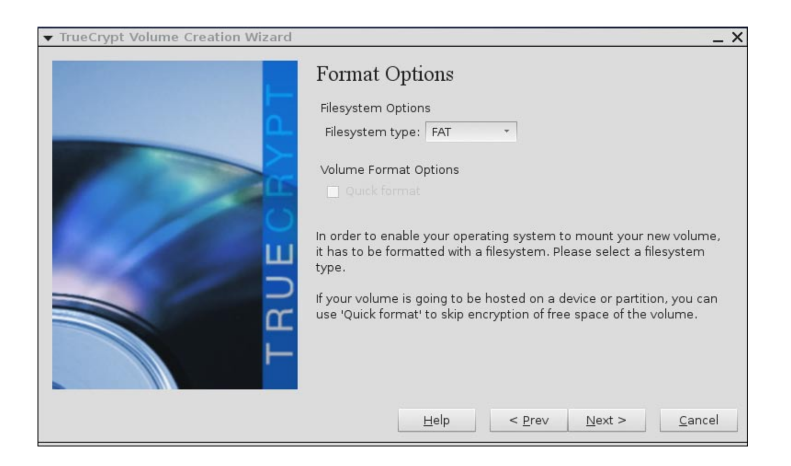


الآن قم بتحديد الحجم المطلوب، ولنفرض ١٠٠ ميجا بايت (جرب أولا).

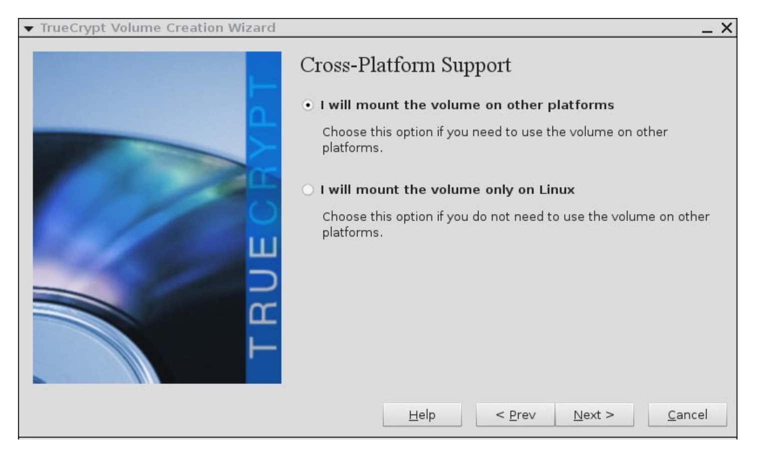


بعد ذلك تابع لعمل الجزء الخاص بكلمة المرور.



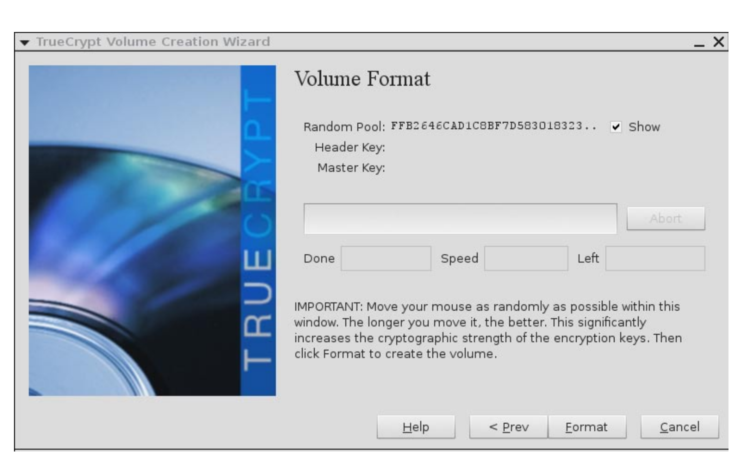


الآن، قم باختيار نظام الملفات الذي تريده لكي يتمكن النظام عندك من عمل ضم Mount له. في حالة كونك تقوم بهذه الخطوات على USB مثلا؛ تستطيع اختيار Quick Format لكي لا تقوم بعمل تشفير للمساحة الفارغة عليه.



ثم انقر على Next مرة أخرى.

إذا كنت ستقوم بعمل ضم Mount لهذا الجزء على أنظمة تشغيل أخرى؛ قم باختيار الخيار الأول، وإلا فاختر الثاني.



وإلا فاختر الخيار الثاني.

الآن، سيطلب منك أن تقوم بتحريك مؤشر الفأرة بأكبر قدر ممكن وبشكل عشوائي لكي تحصل على أفضل سرية/تشفير ممكن للمفاتيح.
انقر على Format لتتم عملية التهيئة.

بعد أن انتهيت من إنشائه، تستطيع عمل ضم Mount له من خلال TrueCrypt، وذلك عن طريق اختيار Mount.

إن شاء الله سنتناول المزيد حول تشفير البيانات في العدد القادم.

الموقع الرسمي للبرنامج:

http://www.truecrypt.org

كيف تستعيد السيطرة على خادمك المخترق!

إعداد : سامر حداد

إن أي مدير للنظام سيحاول جاهداً وفي كل الأيام الحفاظ على خادمه أو نظامه آمناً وسليماً من محاولات الإختراق ، ويحاول تفادي التعرض إلى دخول غير مشروع وعمليات تخريبية لنظامه الذي يتولى إدارته، ونحن هنا نتمنى أن لا يضطر أي واحد فينا في يوم من الأيام إلى إستعادة السيطرة على خادمه المخترق من قبل بعض المخربين، ولكننا وفي كل الأحوال سنقوم بعرض بعض الطرق والمعلومات المفيدة في حالة حدوث مثل هذا النوع من المشاكل الأمنية في محاولة منا لمساعدة مدير النظام على اختيار الطريقة الأنسب والأجدر إتباعها في هذه الحالة لاستعادة نظامه المكشوف والمخترق.



إن عمليات الإختراق تختلف وتتنوع كثيراً تباعاً لنوع الثغرة المستغلة أو طريقة الدخول للنظام وتختلف بدرجة المهارات الموجودة لدى المخترق ولا يمكن لأي شخص حصرها في موضوع واحد ومنها موضوعنا هذا أيضا، ولكن ورغم هذا الأمر إلا أن القواعد الأساسية التي سنوضحها هنا قد تكون بمثابة نقطة إنطلاق للعديد منا لتطوير المهارات والخبرات اللازمة لوضع خطة الإستعادة الخاصة بك.

في معظم الحالات التي يتعرض بها نظامك إلى اختراق من مستوى المستخدم الجذر (أي أن المخترق تمكن من الوصول لصلاحيات المستخدم الجذر root على الخادم أو النظام) فإنه يطلب إليك إعادة تنصيب النظام وجميع الخدمات من جديد و بشكل كامل ومن ثم البدء من جديد، والسبب في ذلك يعود إلى صعوبة اكتشاف جميع الملفات المخفية والتي لربما قام المخترق بزرعها داخل نظامك وفي أماكن يصعب الوصول إليها أو حتى إكتشافها، ولكي يتمكن من إعادة الدخول إلى نظامك في أي وقت آخر ودون الحاجة إلى إعادة الخطوات التي قام بها للوصول غير المشروع للنظام، وهذه الخطوة تسمى بـ Maintain Access وهي الخطوة التي تلي عملية إختراق النظام مباشرة وتأتي بعدها عملية إخفاء الآثار Erasing Tracks .

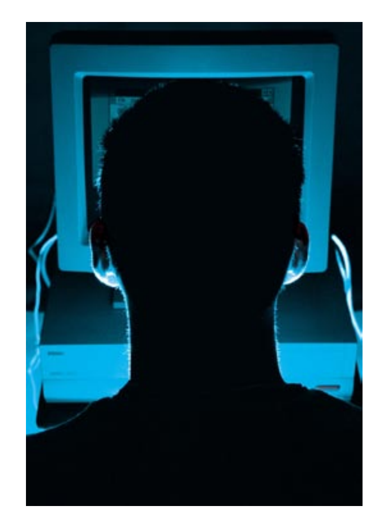
إن ما ذكرناه أعلاه هو أمر صحيح ومحبب دوماً إن كنت تستطيع تحمل نتائج هذا الأمر من فقدان للبيانات وإعادة للإعدادات من جديد، ولكن النظام المستغل هنا أو الذي تعرض لعملية الإختراق قد يكون مرجعاً مهماً لوجود العديد من المعلومات المهمة فيه والتي ستساعد لفهم عملية الهجوم وكيفية التصدي لها في المستقبل.

فيما يلي سنقوم بترتيب الخطوات التي يجب اتباعها في حالة تعرض نظامك للاختراق وسنقوم بتوضيح كل منها بشكل كامل.

لا تفزع! حافظ على هدوئك وقم بتجهيز خطة عمل :

حسناً ، لقد اكتشفت للتو بأن نظامك قد تعرض للإختراق، وحتى لو كان هذا الأمر فعلا سيعرضك الكثيرين للفزع وربما التخبط والتسرع في اتخاذ الإجراءات إلا أنه ومن المطلوب في مثل هذه الحالات أن تحافظ على هدوئك ورباطة جأشك للقيام باستعادة السيطرة على نظامك المكشوف، ولا تتسرع باتخاذ أي خطوة قد تندم عليها لاحقاً. ربما قد يقول البعض منا أن هذا الأمر ليس صحيحاً، فأنت بحاجة للتصرف بسرعة للحيلولة دون تفاقم الأمور، ولكننا سنوضح لماذا قد يكون من الضروري التحلي بالصبر والتفكير الصحيح وتحديد خطة العمل قبل الشروع بالتطبيق، فقد يكون خادمك قد تعرض للاختراق وقد حصل ما حصل، فردة فعلك سواء خلال الثواني الأولى أو الدقائق القليلة التالية قد لا تشكل فرقاً كبيراً في بعض الحالات.

إن كانت لديك خطة عمل قمت بإعدادها مسبقاً (كما هو الهدف الأساسي من هذا المقال) فعليك الشروع بالتطبيق مباشرة دون تأخير ودون تضييع أي وقت، ولكن إن كنت لم تقم بإعدادها مسبقاً فعليك التريث والتفكير في الخطوات التالية التي يجب أن تقوم بها.
إحدى الحالات التي قد يسببها التسرع في التعامل مع عملية الإختراق قد تكون في أن النظام قد لا يزال يكون تحت عملية الإختراق أو أن المخترق لا يزال متواجداً في نظامك، فعندما تشرع بعملية killall لكل السكريبتات التي قام المخترق بتنفيذها على خادمك وتبدأ بالتفكير فيما ستفعله لاحقاً، يكون المخترق قد اكتشف أنك علمت بأمر وصوله غير المشروع للنظام (ربما من خلال الـ irc bot الذي يستخدمه أو غيره) مما قد يشعره بالإنزعاج ويقوم بمسح نظامك كاملاً (بأمر مثل cat /dev/urandom > /dev/sda) وهذا بالطبع ما لا نريده، لذا فأن الهدف الأساسي من هذه النقطة الأولى هي أن لا يكون هناك أي تأخير في تتالي وتتابع الخطوات، وأن تكون قد أعددت خطتك مسبقاً وتنتقل من خطوة للتي تليها بسرعة ودون تردد.



قم بفصل النظام عن الشبكة:

هذا الإجراء قد لا يكون ممكناً دائماً، ولكن وفي حالة وجود إتصال مباشر بينك وبين الخادم أو في حالة كان خادمك مداراً عن بعد في مركز بيانات Data Center يوفر طريقة اتصال من محطة طرفية (مثل أي remote console أو KVM أو بطاقة DRAC كالتي توجد في خادمات Dell) فهذا الإجراء هو الذي يجب عمله مباشرة. فعليك الإتصال بخادمك من خلالها وإيقاف عمل كرت الشبكة.
في حالة عدم توفر الطريقة التي ستقوم من خلالها بالوصول إلى خادمك المدار عن بعد لايقاف عمل كرت الشبكة فيمكنك مثلا أن تستأجر KVM بشكل مؤقت من مركز البيانات الذين يستضيفون خادمك لديهم ، أو أن تقوم بعمل بعض الإعدادات للجدار الناري iptables والتي ستمنع أي إتصال لأي عنوان IP ما عدا العنوان الخاص بك. بعد عمل هذه الخطوة فأن خادمك سيظهر للجميع على أنه قد أوقف عن العمل وبالطبع سيكون من ضمنهم المخترق نفسه.

إكتشف الطريقة التي استخدمت لاختراق نظامك:

هذا الإجراء قد يعتبر الأهم من ضمن جميع الإجراءات الأخرى ويفترض بك معرفة الاجابة عن التساؤل التالي قبل الإنتقال للخطوة التالية: كيف تعرض نظامي للاختراق؟! كما أن هذه الخطوة قد تكون الأطول والأكثر استهلاكاً للوقت حيث أن طرق الإختراق واستغلال الثغرات كثيرة جداً ومتنوعة وقد يصعب معرفتها بسرعة، ولكن عدم استطاعتك لايجاد الطريقة التي استخدمها المخترق للدخول إلى نظامك وقيامك بإستعادة النظام وتشغيله من جديد قد يعرض نظامك للاختراق من جديد وخلال دقائق قليلة، وفي هذه المرة قد لا يكون الوقت لصالحك وقد لا تجد أي شيء موجود على نظامك لكي تستعيده من جديد! ولكن ورغم عدم وجود طرق ثابتة لمعرفة كيفية حدوث الإستغلال إلا أننا سنعرض بعضا من الطرق المفيدة في هذا المجال:

* تبعاً للأدوات التي تستعملها عليك معرفة الملفات التي تم رفعها على نظامك، إما باستعمال أدوات مثل Tripwire الذي يساعد في معرفة أي من الملفات قد تم تعديلها أو إضافتها للنظام ، او من خلال استعمال أمر بسيط مثل find للبحث عن الملفات التي تم تعديلها خلال دقائق أو أيام ، وللبحث عن الملفات ذات الصلاحيات المريبة (مثل التي تم تفعيل خاصية SUID عليها مثلاً)

* من هو المستخدم الذي يملك الملفات المرفوعة على خادمك أو بمعنى آخر من هو الـ File Owner . قد يساعدك هذا الأمر في تحديد التطبيق أو الخدمة التي تم استغلالها لاختراق النظام، فعلى سبيل المثال الملفات التي تم رفعها باستخدام المستخدم apache سوف يشير إلى أن خدمة الويب قد تم استغلالها لعمل هذا الوصول غير المشروع.

* تفحص الملفات التي تم رفعها على خادمك وقم بقراءة محتوياتها جيداً، فمثلا قد يستخدم المخترق نفس الثغرة التي استخدمها للوصول إلى نظامك للوصول لأنظمة أخرى من خلالك، وهذا قد يساعدك على اكتشاف الثغرة التي استغلها المخترق للوصول إلى نظامك.



* قم باستخدام برامج كشف الـrootkits مثل برنامج rkhunter و chkrootkit في محاولة لكشف أي ملفات أو مكونات نظام تم حقنها في نواة نظام التشغيل.

* إطلع على ملفات السجلات لديك log files وبالتأكيد وبعد قيامك بكل الخطوات السابقة يمكنك حصر أسباب المشكلة وبالتالي التخفيف من حجم عملية البحث في ملفات السجل الكبيرة.

بعد كل تلك العمليات والإجراءات في محاولتك لتحديد سبب وطريقة الإختراق فإننا نأمل أنك قد نجحت في تحديد الطريقة التي تم بها استغلال خادمك، ومرة أخرى نذكر أن هذا سيختلف باختلاف الطريقة التي تمت بها عملية الإختراق.

إن أغلب عمليات الإختراق التي تحصل في يومنا هذه تعود إلى ثغرة ما في تطبيقات الويب الموجودة على الخادم، فيستغلها المخترق لتنفيذ سكريبتات عديدة، ولكنك أيضا قد تواجه مشكلة أكبر عند وصول مخترق متخصص في أنوية النظم فيقوم بتحميل kernel module لنواة نظامك لكي يخفي أي آثار له مما يجعل من الصعب جداً تحديد أو حتى رؤية الإختراق!

- أوقف كل السكريبتات وأزل ملفات المخترق:



عليك الآن وقف عمل جميع السكريبتات التي نفذها المخترق وحذف جميع الملفات الخاصة به، أو تخزينها في مكان آخر لعمل المزيد من التحريات عليها في وقت لاحق.

في هذه اللحظة نحن لا نحتاج تلك السكريبتات لتبقى تعمل على نظامك حيث قمنا بالحصول على العديد من المعلومات من خلالها. ولا تنسى أن النظام لا يزال غير متوفرا للعالم الخارجي أيضا.

لا تنسى أن تتطلع على الأماكن التي لربما قام المخترق بوضع أوامره الخاصة التي ستقوم بتشغيل ملفاته وسكريبتاته بعد إعادة التشغيل مثل: cron tabs ، rc.local ، init scripts ، وغيرها ...

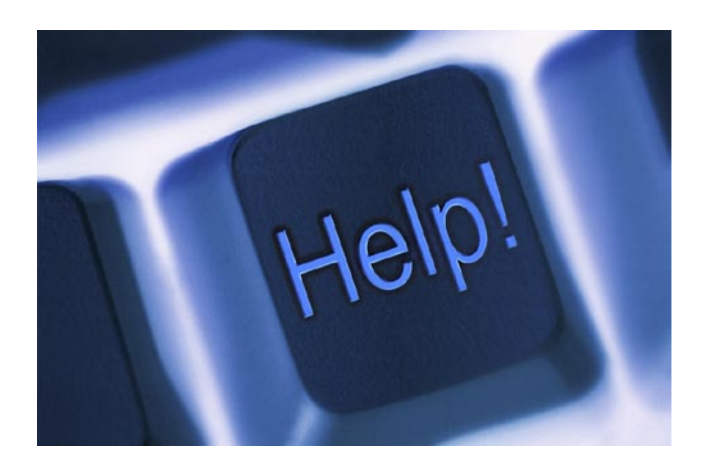
أعد تشغيل جميع الخدمات التي لم تتأثر بالإختراق:

بعدما علمنا ما هي الخدمة التي تم اختراق النظام من خلالها يمكننا الآن إعادة تشغيل باقي الخدمات الاخرى التي لم يكن لها دور في تلك العملية مع الإبقاء على الخدمة المستغلة موقفة عن العمل. قم بإعادة تشغيل كرت الشبكة وباقي الخدمات غير المستغلة في الإختراق.

مثال: إذا كانت الخدمة المستغلة في الإختراق هي خدمة الويب Web فعليك ايقافها عن العمل مع إعادة تشغيل الخدمات الأخرى كخدمة البريد Mail وخادم الإسم DNS وغيرها لكي نقلل من زمن تعطل النظام.

قم بإصلاح الثغرة في الخدمة التي سببت الإستغلال:

قبل أن تقوم بتشغيل الخدمة التي تسببت في إستغلال النظام عليك أن تتأكد من إصلاح الخلل في تلك الخدمة والتي تسببت إحدى...



... إحدى ثغراتها في إختراق نظامك قبل أن تقوم بتشغيل الخدمة للعامة مجددا وذلك حسب طبيعة الثغرة الموجودة في تلك الخدمة. قد تحتاج لعمل إحدى أو جميع التالية:

- ترقيع الثغرة في الخدمة.
- تحديث تطبيق الويب المستخدم (أو ايقافه مؤقتاً).
- كتابة بعض القواعد لصده عن بعض الأمور (مثال: يمكن استخدام mod_security في حالة عدم وجود تحديث أو ترقيع لثغرة تطبيق الويب المستغل).

أعد تشغيل الخدمة بعض تصليحها:

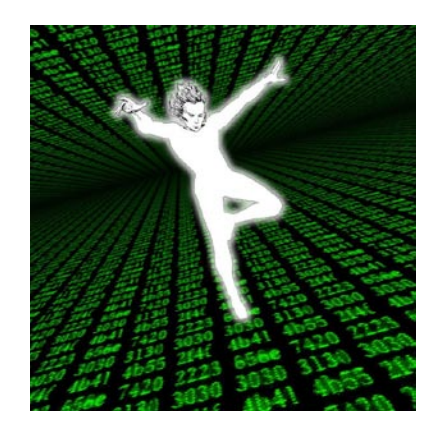
بعد إصلاح الخلل يمكنك إعادة اشغيل الخدمة التي تم استغلالها ولكن بحذر.

راقب النظام عن كثب:

الأن عليك بمراقبة نظامك عن كثب للتأكد أن الثغرة قد تم إغلاقها والتصحيح الذي قمت به يعمل بشكل جيد. يبدو أنه وبشكل شبه مؤكد فإن المخترق سيقوم بمحاولة الوصول مرة أخرى لنظامك للتأكد أنك قد نجحت في تصويب الوضع أم أن النظام لا يزال قابلاً للإستغلال. وقد يرى أن النظام قد ضاع من يده بعد أن قام باختراقه فيحاول مرة أخرى وبجهد أكبر هذه المرة. لذا فإن مراقبة النظام من أي محاولات دخول غير مشروعة ستساعدك على التصدي بشكل أفضل هذه المرة. عند ملاحظتك لأي مشكلة أو لأي شيء غير طبيعي فعليك إيقاف الخدمة ومحاولة البدء من جديد.

الخاتمة:

لعلك لاحظت أخي العزيز أن الخطوات أعلاه قد لا تكون فعالة في كل الحالات وذلك لاختلاف طريقة الهجوم والإستغلال الذي قد يحصل للأنظمة والخوادم، ولكنها يمكن أن تستخدم كقاعدة أساسية للإنطلاق منها وستساعدك بالتأكيد لمواجهة أي خطر غير متوقع حيث أنه قد أصبحت لديك خطة ستعمل عليها لمواجهة مثل هذه الحوادث. وتذكر أن الحماية المطلقة في عالم الحواسيب ما هو إلا ضرب من الخيال!



فريق عمل المجلة:

رئيس التحرير: سامر حداد — GreyHunter

التدقيق اللغوي:

محمود سعيد — محمود سعيد

مأمون ديرانيه — مأمون

هيئة التحرير:

مؤيد السعدي — alsadi

روضة الصوابني — raoudha

بدري دركوش — Free-Programmer

أحمد السيد محمود — أحمد السيد !

يونس بوطيور — niceboy

حسام الدين قريوج — houcemeddine

صبري صالح — KING SABRI

محمد الخياري — knoppix_dark

علي الشمري — B!n@ry

مسلم عادل — مسلم عادل

تصميم وإخراج: سامر حداد — GreyHunter



